НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ “ВАСИЛ ЛЕВСКИ”

ФАКУЛТЕТ “АРТИЛЕРИЯ, ПВО И КИС”

Катедра “Информационна сигурност”

Н А У Ч Н А К О Н Ф Е Р Е Н Ц И Я 2 0 1 4

НОВАТА ПАРАДИГМА ЗА СИГУРНОСТ В КИБЕРПРОСТРАНСТВОТО

СБОРНИК НАУЧНИ ТРУДОВЕ

ШУМЕН
2014

КЪМ ЧИТАТЕЛИТЕ ...

Сборникът научни трудове е съставен от докладите, изнесени на научна конференция на тема „Защитата на личните данни в контекста на националната сигурност", проведена във Факултет "Артилерия, противовъздушна отбрана и комуникационни и информационни системи" към Националния военен университет "Васил Левски" - гр. Шумен, на 5 и 6 юни 2014 г.

Докладите са представени за издаване от авторите без допълнително редактиране от издателите. Отговорността за фактологическите, технически, езикови грешки и произтичащите от това последствия носят изцяло авторите.

Съгласно чл. 31 от Закона за защита на класифицираната информация авторите сами определят грифа на докладите си и носят лична отговорност за публикуване на класифицирана информация в тях.

От редакционната колегия

©НВУ "В. Левски" – Факултет "Артилерия, ПВО и КИС"
Шумен, 2014.
c/o Jusautor, Shumen

ISBN 978-954-9681-49-9

СЪДЪРЖАНИЕ

ПЛЕНАРНА СЕСИЯ 7

ПРИВЕТСТВИЕ КЪМ УЧАСТНИЦИТЕ В КОНФЕРЕНЦИЯТА 7

М. П. Млеченков, НОВИТЕ ИЗМЕРЕНИЯ НА ИНФОРМАЦИОННАТА ВОЙНА 10

В. Ст. Ризов, НАЦИОНАЛНАТА СТРАТЕГИЯ ЗА КИБЕРСИГУРНОСТ – ИНСТРУМЕНТ ЗА ГАРАНТИРАНЕ НА СВОБОДНО И БЕЗОПАСНО КИБЕРПРОСТРАНСТВО 38

Д. А. Николова, ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ В КИБЕРПРОСТРАНСТВОТО 45

Д. Л. Полимирова, КИБЕР АТАКИ И СЪВРЕМЕННИ ПОДХОДИ ЗА ЗАЩИТА..... 53

Д. Кънев, ЕНЕРГИЙНА КРИТИЧНА ИНФРАСТРУКТУРА – МЕТОДОЛОГИЯ ЗА ОПРЕДЕЛЯНЕ РИСКА НА ОБЕКТИТЕ 59

ДЪРЖАВА И СИГУРНОСТ 62

М. Бонева, ХРАНИТЕЛНИ ДОБАВКИ И СИГУРНОСТ..... 62

М. Бонева, ТОКСИЧНИ МЕТАЛИ 70

М. Бонева, Георги Колев, СОЦИАЛНА МАНИПУЛАЦИЯ И СИГУРНОСТ 75

Св. Пл. Илиев, Н. Й. Досев, Хр. А. Христов, ПРЕДАВАНЕ НА ТАЙНИ СЪОБЩЕНИЯ ЧРЕЗ СТЕГАНОГРАФСКИ СПОСОБИ ВЪВ FACEBOOK И GOOGLE+ 82

К. И. Кръстев, Х. А. Христов, ЕВОЛЮЦИЯ В СХВАЩАНИЯТА ЗА СИГУРНОСТТА 88

Кр. М. Марков, ПРОБЛЕМЪТ ЗА ДОМАШНОТО НАСИЛИЕ..... 97

Кр. М. Марков, ЗА СУИЦИДНОТО ПОВЕДЕНИЕ.....101

Кр. М. Марков, ПСИХОЛОГИЧЕСКИ АСПЕКТИ НА КОРПОРАТИВНАТА СИГУРНОСТ ПРИ ВОДЕНЕ НА ПРЕГОВОРИ.....109

Ч. Л. Милков, СПЕЦИФИКА НА МИГРАЦИОННИТЕ ПРОЦЕСИ В ЕВРОПА ПРЕЗ XXI ВЕК.....114

Ч. Л. Милков, ДОБРИ ПРАКТИКИ НА АНГЛИЯ В ОБЛАСТТА НА МИГРАЦИОННАТА ПОЛИТИКА И ВЪЗМОЖНОСТИТЕ ЗА ПРИЛОЖЕНИЕТО ИМ В БЪЛГАРИЯ.....121

Ч. Л. Милков, ВАИМООТНОШЕНИЯТА „ДЪРЖАВА-ГРАЖДАНСКО ОБЩЕСТВО“.....128

М. Митевска-Енчева, СТАБИЛНОСТ И ИЗМЕНЧИВОСТ В ОРГАНИЗАЦИОННИТЕ ЦЕННОСТИ.....140

М. Митевска-Енчева, СИГУРНОСТ И КРИЗА В ДОМИНИРАЩИТЕ ЦЕННОСТНИ ПРЕДПОЧИТАНИЯ В ОРГАНИЗАЦИОННА СРЕДА.....148

М. Митевска-Енчева, ЕФЕКТИ НА ОРГАНИЗАЦИОННИ ЦЕННОСТИ ВЪРХУ ПРОЯВИТЕ НА ПРОСОЦИАЛНОТО ПОВЕДЕНИЕ.....154

Ст. Ст. Станев, СПЕКУЛАТИВНА АТАКА СРЕЩУ ФИКСИРАНИЯ ВАЛУТЕН КУРС. РЕАЛНА ЗАПЛАХА ЗА ФИНАНСОВАТА СИГУРНОСТ НА Р. БЪЛГАРИЯ ПРИ СЪВРЕМЕННИТЕ УСЛОВИЯ.....160

Ст. Ст. Станев, ФИНАНСОВА СИГУРНОСТ НА ДЪРЖАВАТА - ПОДСИСТЕМА НА СИСТЕМАТА ЗА НАЦИОНАЛНА СИГУРНОСТ ...164

В. Д. Стоянов, Хр. А. Христов, АСПЕКТИ НА СИГУРНОСТТА НА БАНКОВИТЕ ТРАНЗАКЦИИ, ОСЪЩЕСТВЯВАНИ ЧРЕЗ ПОС ТЕРМИНАЛ, ДЕБИТНИ И КРЕДИТНИ КАРТИ 169

С. Г. Тонев, ПРОЦЕС НА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ ПРИ КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ КАТО ЕЛЕМЕНТ ОТ НАЦИОНАЛНАТА СИСТЕМА ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА.....175

С. Г. Тонев, ОБЩИ ПОЛОЖЕНИЯ - ПРАВНИ СТАНДАРТИ НА КОМПЮТЪРНИ ПРЕСТЪПЛЕНИЯ 183

В. П. Петров, КОНТРАБАНДАТА И НЕЛЕГАЛНОТО РАЗПРОСТРАНЕНИЕ НА НАРКОТИЦИ В РЕПУБЛИКА БЪЛГАРИЯ...190

В. П. Петров, КОНТРАБАНДАТА И НЕЗАКОННАТА ТЪРГОВИЯ С ОРЪЖИЕ.....197

В. П. Петров, ЯВЛЕНИЕТО НЕЗАКОНЕН ТРАФИК НА ХОРА 206

С. Р. Велков, ВЪЗНИКВАНЕ И РАЗВИТИЕ НА ОНЛАЙН РЕКЛАМАТА КАТО ЕЛЕМЕНТ НА МАРКЕТИНГА 213

С. Р. Велков, ЕВОЛЮЦИЯ НА НАЧИНИТЕ ЗА ПЛАЩАНЕ НА ОНЛАЙН РЕКЛАМАТА 221

С. Р. Велков, ВЪЗМОЖНОСТИ ЗА ПРИЛАГАНЕ НА НОВИ ТЕХНОЛОГИИ 225

З. Ю. Кузманов, ПОЛИТИКИ НА РУСКАТА ФЕДЕРАЦИЯ ПРИ УПРАВЛЕНИЕ НА КРИЗИ 233

З. Ю. Кузманов, ПОЛИТИКИ НА ЕВРОПЕЙСКИЯ СЪЮЗ ПРИ УПРАВЛЕНИЕ НА КРИЗИ 236

З. Ю. Кузманов, ПОЛИТИКИ НА СЪЕДИНЕНИТЕ АМЕРИКАНСКИ ЩАТИ ПРИ УПРАВЛЕНИЕ НА КРИЗИ 240

ИНФОРМАЦИОННА СИГУРНОСТ.....244

Р. Ст. Гюров, МОДЕЛ ЗА ОЦЕНКА НА ВЪНШНАТА СРЕДА ПРИ АНАЛИЗА НА КОРПОРАТИВНИЯ РИСК.....244

К. И. Кръстев, *Ст. С. Станев,* СТЕГАНОЛОГИЧНА ЗАЩИТА НА ИНФОРМАЦИЯТА В КОНТЕКСТА НА КОНТРАРАЗУЗНАВАТЕЛНОТО ОСИГУРЯВАНЕ НА СИГУРНОСТТА НА ВОЙСКОВИ КОНТИНГЕНТ ЗАД ГРАНИЦА.....252

Ж. Н. Ташева, Р. А. Богданов, АНОНИМНА СИСТЕМА ЗА КОМУНИКАЦИИ В КИБЕРПРОСТРАНСТВОТО, ИЗПОЛЗВАЩА ПРОТОКОЛА TOR 259

Г. Р. Иванов, КОНЦЕПТУАЛНИ АСПЕКТИ НА КИБЕРСИГУРНОСТТА 266

М. Х. Ламбева, ПРИЛОЖЕНИЕ НА FPGA ЗА ИЗГРАЖДАНЕ НА УСТРОЙСТВА ЗА КРИПТИРАНЕ НА ДАННИ 271

Д. Т. Дойчинов, ЕДИН МЕТОД ЗА ОЦЕНКА НА ЗАПЛАХИТЕ ЗА СИГУРНОСТТА НА ИНФОРМАЦИЯТА 277

Л. Г. Николов, К. О. Славянов, ЕФЕКТИВНОСТ НА СОФТУЕР ЗА КОМУНИКАЦИОННО РАЗУЗНАВАНЕ 283

В. Т. Стоянова, СТЕГАНОГРАФИЯТА В СОЦИАЛНИТЕ МРЕЖИ И В ОНЛАЙН СПОДЕЛЯНЕТО НА СНИМКИ 291

Ат. И. Начев, Д. Г. Чобанов, МЕТОД ЗА ЧЕСТОТНО РАЗДЕЛЯНЕ НА КАНАЛА ПРИ СИНУСОИДАЛНИ НОСЕЩИ 297

Д. Г. Чобанов, МОДЕЛ НА СИСТЕМА С ЧЕСТОТНО РАЗДЕЛЯНЕ НА КАНАЛА ПРИ СИНУСОИДАЛНИ НОСЕЩИ И АМПЛИТУДНО–ФАЗОВА КОРЕЛАЦИОННА МОДУЛАЦИЯ 300

Д. Г. Чобанов, МОДЕЛ НА СИСТЕМА С ЧЕСТОТНО РАЗДЕЛЯНЕ НА КАНАЛА ПРИ СИНУСОИДАЛНИ НОСЕЩИ 303

Н. Ж. Кулев СПЕКТРАЛЕН АНАЛИЗ НА СЛОЖЕН (ШУМОПОДОБЕН) РАДИОКАЦИОНЕН СИГНАЛ 306

СТУДЕНТСКО-ДОКТОРАНТСКА СЕКЦИЯ 310

А. И. Иванова, П. С. Великов, ФИРМЕНА ПОЛИТИКА „ДОНЕСИ СВОЕТО УСТРОЙСТВО“ И ОСИГУРЯВАНЕ НА ОБЛАЧНО БАЗИРАНИ УСЛУГИ 310

Хр. А. Десев, Св. С. Камджалов, СИСТЕМИ ОТ ТЕХНИЧЕСКИ СРЕДСТВА ЗА ПОЛУЧАВАНЕ НА РАЗУЗНАВАТЕЛНА ИНФОРМАЦИЯ ОТ КОМПЮТЪРНИ МРЕЖИ 318

В. П. Крумов, МОДЕЛИ ПРИ УПРАВЛЕНИЕТО НА ИНЦИДЕНТИ В ИНФОРМАЦИОННАТА СИГУРНОСТ 324

ПЛЕНАРНА СЕСИЯ

ПРИВЕТСТВИЕ КЪМ УЧАСТНИЦИТЕ В КОНФЕРЕНЦИЯТА
от декана на Факултет „Артилерия, противовъздушна отбрана и комуникационни и информационни системи" – Шумен
полковник доцент доктор Нелко Ненов

Уважаеми госпожи и господа,
Уважаеми господин Полковник,
Уважаеми офицери, курсанти, студенти, докторанти и специализанти,
Скъпи гости,

Добре дошли на ежегодната конференция по проблемите на информационната сигурност, организирана от Националния военен университет „Васил Левски", Факултет „Артилерия, ПВО и КИС" в Шумен.

Конференцията се провежда с цел да развие, обогати и сподели знания, умения, опит и научни постижения в сектора сигурност. И тази година конференцията организираме съвместно с нашите партньори и колеги, с които работим няколко години поред.

Вече осем години в Шумен провеждаме обучение на студенти, специализанти и докторанти в професионално направление „Национална сигурност" по специалност „Административна и информационна сигурност". Дългогодишни са нашите традиции в обучение на кадри с висше образование по в професионално направление „Комуникационна и компютърна техника" по специалност „Компютърни системи и технологии", „Комуникационна техника и технологии", а от скоро и по „Компютърни технологии за проектиране".

Към настоящия момент във Военния факултет в Шумен се обучават общо 444 обучаеми - студенти и докторанти, без да смятаме курсантите и специализантите. Част от тях присъстват днес на конференцията, други ще изнесат доклади в студентско-докторантската научна секция.

За тези години смея да твърдя, че натрупахме значителен опит в областта на информационните аспекти на сигурността, не само в обучението на експерти, но и по отношение участие в научни и образователни проекти.

Госпожи и господа,

Тази година конференцията провеждаме под надслов „Новата парадигма за сигурност в киберпространството". Темата е изключително актуална поради ред причини, свързани с предизвикателствата в съвременния свят.

За посрещане на киберзаплахите днес е необходим интердисциплинарен подход, който да осигури всеобхватно решаване на проблема, с привличане експертния състав на всички институции, както в национален, така и в съюзен контекст. Едно от основните предизвикателства в днешния дигитален свят преминава през фокуса на запазване на личното пространство и технологичната надеждност в киберсвета, създаване на потребителска дигитална култура и, разбира се, на норми на контрол в постоянно еволюиращата среда за сигурност.

Темата киберсигурност зае приоритетно място в срещата на най-високо равнище в ЕС през 2012 г. В резултат на това Европейската комисия се задейства и пред-

стави стратегия за киберсигурност и директива за сигурността на информационните системи.

България също се ангажира в този процес. В момента се разработва национална стратегия за киберсигурността на информационните потоци и базата данни, която максимално да защити информацията.

Целта, която си поставяме на настоящия форум, е да анализираме най-новите европейски и международни стратегии и политики в областта на киберсигурността, перспективите пред националната стратегия за киберсигурност, изграждането на система за ранно реагиране, както и споделяне на най-добрите решения и практики в областта на информационната сигурност.

За мен е чест и удоволствие да обявя, че съорганизатори на настоящата конференция са Държавна агенция „Национална сигурност", Държавната комисия по сигурността на информацията, Комисията за защита на личните данни, Дирекция „Комуникационни и информационни системи" – МО, Дирекция „Сигурност на информацията" - МО и Институтът по отбрана „Проф. Цветан Лазаров.

В научния форум участват и представители на Националната лаборатория по компютърна вирусология – БАН, Министерство на вътрешните работи, Държавна агенция „Технически операции", Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи" към Министерството на транспорта, информационните технологии и съобщенията, Министерството на икономиката и енергетиката, Служба „Военна полиция" – МО, Фондация „Право и интернет", Международна академия за обучение по киберразследвания.

Изключително важно за нас е участието на представителите на водещи компании в сектора на информационните и комуникационни технологии, като Роде и Шварц и Сиско.

В конференцията участват колеги преподаватели и изследователи от ВА „Раковски" – София, Шуменския университет „Епископ Константин Преславски", Университета по библиотекознание и информационни технологии и други.

Госпожи и господа,

За мен е чест да обявя нашите гости:

- Кмета на община Шумен – г-н Красимир Костов;
- Областния управител – г-н Венцислав Венков;
- полковник Емил Шошев – командир на Стационарната комуникационна и информационна система на БА, който с Указ на президента на Република България, считано 29 юли 2014 г. е повишен в звание бригаден генерал и назначен на длъжност директор на Дирекция „Комуникационни и информационни системи" в МО;
- г-н Васил Ризов – заместник-председател на Държавната комисия по сигурността на информацията;
- г-н Иван Иванов – член на Държавната комисия по сигурността на информацията;
- д-р Румен Гюров – главен експерт в дирекция „Защита на класифицираната информация" в Държавната комисия по сигурността на информацията;
- д-р Николай Николов – началник на отдел „Киберсигурност" в Държавна агенция „Национална сигурност";
- комисар Валентин Александров – директор на Областна дирекция на МВР – Шумен;

- полк. Йосиф Атанасов – заместник - директор на дирекция „Сигурност на информацията" в МО;

- подп. Атанас Атанасов – началник на отдел „Информационна сигурност и киберзащита" в дирекция „Сигурност на информацията в МО;

- доц. д-р Димитрина Полимирова – директор на Националната лаборатория по компютърна вирусология – БАН;

- г-жа Весела Христова – директор на дирекция „Сигурност на информацията" в Държавна агенция „Технически операции";

- г-н Стайко Христов – главен експерт, преподавател в дирекция „Научно приложни дейности" в Държавна агенция „Технически операции";

- г-н Васил Грънчаров – директор на Национален център за реакция при инциденти в информационната сигурност в Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи" към министерството на Транспорта информационните технологии и съобщения;

- г-н Димчо Кънев – началник на отдел „Защита на критичната инфраструктура" в Министерството на икономиката и енергетиката;

- г-жа Десислава Николова, старши експерт в отдел „Правни становища и международно сътрудничество" в Комисия за защита на личните данни;

- г-жа Наталия Николова, младши експерт в отдел „Правни становища и международно сътрудничество" в Комисия за защита на личните данни;

- подп. доц. д-р Николай Стоянов – началник на научно направление "Защита на информацията" в Института по отбрана „Проф. Цветан Лазаров - МО;

- м-р Владимир Владимиров – Служба „Военна полиция" – МО;

- адвокат Десислава Кръстева - старши експерт във фондация „Право и интернет";

- г-н Любомир Пиперов – изпълнителен директор на „Роде и Шварц – България";

- г-н Пламен Пунчев – системен инженер в „Сиско системс" – България;

- г-н Пламен Жечев – представител на „Сиско системс" – България;

Благодаря на всички гости, че уважиха нашата покана и се включиха в работата на конференцията.

Госпожи и господа,

По време на пленарната сесия на форума ще имате възможността да се запознаете с актуалните постановки, свързани с новите измерения на информационната война, държавната политика в сферата сигурността в киберпространството, определена в Националната стратегия за киберсигурност. Тя неизбежно се пречупва през призмата на приоритетите на НАТО и ЕС по киберзащитата. Ще бъдат анализирани въпросите, свързани със защитата на личните данни в киберпространството. Ще бъде предложен модел за изграждане на система за киберсигурност, интегриращ усилията на всички структури, ангажирани в този процес.

Ще бъдат детайлно изследвани еволюцията и съвременните форми на кибератаки, както и подходите за защита от тях.

Важно място е отделено за разкриването на мисията, ролята и функциите на Националния център за реакция при инциденти в информационната сигурност, на защитата на критичната инфраструктура и най-вече критичната информационна инфраструктура.

В отделните научни секции има депозирани интересни доклади и презентации, свързани с използване на стеганографски методи за защита на информацията и

анализ на конкретни стеганографски алгоритми, анализ на сигурността в социалните мрежи и сигурност на банковите транзакции, осъществявани чрез посттерминал, дебитни и кредитни карти.

Ще си сверим часовниците с най-новите разработки на фирмите от ИТ сектора чрез презентациите „Висока степен на защита на комуникациите" на „Роде и Шварц" и „Интелигентни киберзащити в реалния свят" на „Сиско Системс".

За нас е много важно, че в работата на конференцията се включват с доклади и съобщения курсанти, студенти и докторанти. Това е традиция, която се стремим да утвърждаваме и задълбочаваме.

Благодаря на организаторите и съорганизаторите на настоящата конференция.

Желая на всички участници и гости на конференцията успешна и ползотворна работа.

Откривам научната конференция „Новата парадигма за сигурност в киберпространството" – Шумен 2014-та.

НОВИТЕ ИЗМЕРЕНИЯ НА ИНФОРМАЦИОННАТА ВОЙНА

Манол П. Млеченков

„Компютрите – това е оръжие, а линията на фронта минава навсякъде."

Джеймс Адамс
„Следващата световна война",
1998 г.

От началото на новия век светът все повече се глобализира. В него като никога до този момент остро и неотложно се поставя въпроса за сигурността като основен приоритет в отношенията между държавите. Постиженията в областта на информационните технологии поставиха цивилизования свят в състояние, при което информацията се превръща във важен елемент за развитието на обществото. Днес няма сфера от обществения живот, която да не е намерила отражение във виртуалното пространство. Това изисква сигурно кибернетично пространство, безопасни комуникационни и информационни технологии и свързаните с тях инфраструктури.

Глобалната мрежа с огромните си възможности се превръща в един от наймощните инструменти за ускорено развитие на света. Просперитетът, икономическата стабилност и националната сигурност на всяка държава зависят от устойчивото, сигурно и надеждно киберпространство. През последното десетилетие заплахите и атаките в това пространство драстично нарастват и се отразяват на националната сигурност на държавите, бизнеса и личната информация, генерирана, обменяна, обработвана, съхранявана и предоставяна от широк кръг държавни и частни структури и отделни граждани. Това налага политиката за защита на националните информационни активи да се разглежда през призмата на информационната сигурност.

Глобалният характер на интернет и свързаността на мрежите и информационните системи на държавите предполага много от инцидентите в киберпространството да имат последствия, които застрашават националната сигурност, вредят на функционирането на икономиката и излизат извън националните граници. Справянето с нарастналите заплахи за киберсигурността се превръща в предизвикателство пред националната сигурност на държавата и международните процеси. Това може да се постигне чрез промяна на политиките, практиките, разбирането и поведението на организациите и отделните участници в мрежата.

Стремителното разпространение на информационните и телекомуникационните технологии доведе до концентрация на мощ (политическа, икономическа, военна) в няколко световни центрове на влияние. Към настоящия момент лидерската роля при използване на информационните средства безспорно принадлежи на САЩ и американското военно-политическо ръководство разглежда поддържането на лидерството в това направление като най-важен компонент за глобално информационно превъзходство.

Международният стандарт ISO 27032:2012 определя киберпространството като сложна среда, състояща се от взаимодействия между хора, софтуер и услуги, поддържано в световен мащаб чрез разпространение на информационни и комуникационни технологии, устройства и мрежи, то предоставя безкрайни предимства за потребителите. Въпреки това онлайн средата не винаги може да бъде в безопасност.

Киберсигурността има няколко аспекта - сигурност на информацията, сигурност на мрежите, сигурност в интернет и защита на критичната информационна инфраструктура[1].

В този ред на мисли, известният специалист по информационни войни и кибервойни от военното ведомство на САЩ, професор Мартин Либицки казва: „не може да се изключи и военната компонента на националната сигурност, която е в съществена зависимост от защитата на информационните ресурси ... битката, която започва в киберпространството, може да се пренесе в реалния свят с печални за него последствия.”[2]

В доклада се разглеждат четири основни проблема, определящи новите измерения на Информационната война:

1. Концепция за информационните войни в стратегията на САЩ.
2. Новите измерения на информационната война.
3. Киберсигурността в Обединена Европа.
4. Води ли се необявена кибервойна?

1. Концепция за информационните войни в стратегията на САЩ

Нарасналата роля на нетрадиционните силови въздействия, в това число и информационни, ни дава основание да анализираме в исторически аспект зараждането и развитието на схващанията за същността, съдържанието и методите да водене на информационна война (ИВ) и на кибервойната като нейна съставна част.

Един от първите американски автори на концепцията за информационната война Томас Рон през 1976 г. я определи като „съревнование между съперници, кон-

[1] ISO/IEC 27032:2012 Information security – Information Security Techniques – Guidelines for cyber security [Информационни технологии - техники за сигурност – Насоки за киберсигурност].

[2] Libicki M., Cyberdeterrence and cyberwar, RAND Corporation, 2009, ISBN 978-0-8330-4734-2, p. XIX.

куренти или противници на стратегическо, оперативно или тактическо ниво в целия спектър на състоянието на света при криза, ескалация на кризата, конфликт, война, прекратяване на войната, възстановяване на мира с използването на информационни средства за постигане на своите цели." Авторът подчертава, че информационната инфраструктура представлява ключов елемент от американската икономика, но същевременно тя се превръща в уязвима цел, както във военно, така и в мирно време.

При развитието на концепцията за ИВ от 1980 г. е възприето общото схващане, според което, информацията може да бъде както цел, така и оръжие.

По мнението на авторитетните американски експерти Джон Аркуилла[3] и Дейвид Ронфелдт, работещи за корпорация RAND, „информационната революция доведе до появяването на такъв способ за водене на войната, когато ... страната, притежаваща повече знания е способна да расее „облака на войната", създаван от противника и да получи решаващо преимущество.".[4]

Във връзка с поставянето на нови задачи след периода на „Студената война", терминът ИВ е въведен и в документите на Министерството на отбраната на САЩ. Той започва активно да се среща в пресата, особено след операцията „Пустинна буря" (1991 г.), където новите информационни технологии за пръв път са използвани като средство за водене на бойни действия.

Скоро след операция „Пустинна буря" армейското ръководство на САЩ подложи на сериозен анализ опита за постигане на информационно превъзходство на бойното поле. През ноември 1991 г. генерал Глен Отис, бивш командващ на Командването на сухопътните войски по обучението и доктриите, публикува свой труд, в който се казва: „От операция „Пустинна буря" могат да се извлекат много уроци. Някои от тях са нови, другите - стари. Но един урок се явява наистина фундаментален: съдържанието на съвременната война коренно се промени. Тази страна, която спечели информационната кампания – ще победи. Ние демонстрирахме тези уроци на целия свят: информацията е ключа в съвременната война в стратегическо, оперативо, тактическо и техническо отношение."[5]

В директивата на Министерството на отбраната (МО) TS 3600.1, въведена ба 21 декември 1992 г. бяха формулирани основните положения от стратегията за водене на информационна война.[6] Директивата определя информационното противоборство като самостоятелен вид оперативна поддръжка, която се състои от пет основни елемента: психологически операции, противодействие на противниковото разузнаване и осигуряване безопасност за действие на собствените войски, въвеждане на противника в заблуждение, радиоелектронна борба, унищожаване на пунктовете за управление на противника и комуникационната му система.

---

[3] Джон Аркуилла по време на операция „Пустинна буря" е бил съветник на командващия групировката на САЩ в региона генерал Норман Шварцкопф.

RAND Corporation, е „институция с идеална цел, която помага за подобряване на политиката и вземане на решения чрез научни изследвания и анализи."

[4] John J. Arquilla, David F. Ronfeldt. Cyber War is Coming// Comparative Strategy, Vol. 12, 1993.

[5] James Adams. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. New York, 1998. P. 55.

[6] Information Warfare. Directive TS 3600.1. Washington D.C.: U.S. Department of Defense, 21 Dec. 1992.

През август 1995 г. Националния институт по отбраната на САЩ публикува работата на професор Мартин Либицки *„Какво е информационната война?”*. [7] В нея авторът определя *седем форми на информационната война*: командно-управленска, разузнавателно-информационна, психологическа, хакерска, икономическа, електронна и кибервойна – фиг. 1.

Фиг. 1. Съдържание на информационната война

Какво се включва всяка от тези седем форми.

Командно-управленска война, както е определено в американските наставления е насочена за „обезглавяване” на системата за управление на войските на противника, т.е. за физическо унищожаване на центровете и пунктовете за управление, нарушение на системата за управление на войските, комуникационните линии и като цяло системата за управление на стратегическо, оперативно или тактическо ниво.

Разузнавателно-информационна война. Техническа основа на тази война са средствата за разузнаване, комуникации и различен тип управление, осигуряващи добиване на информация за противника на цялата дълбочина на неговото оперативно построение, предаването и в реален мащаб на времето на информационно-аналитичните системи на своите войски и на тази основа формиране на управля-

[7] Libicki M. What is Information Warfare. Santa Monica: RAND, 1995.

ващи въздействия. В едно бъдещо бойно поле ще господстват не „платформи, конструктивно съединяващи оператори, сензори и въоръжение", а „отделни системи, електронно свързани помежду си." Тези технологии на този принцип се основава стратегията за „мрежовоцентричните операции."

Електронната война като форма на информационната война се води в сферата на комуникациите и включва радиоелектронната борба и криптографска война. Това не е нова форма на водене на военни действия. Тя предполага борба с РЛС на противника, нарушаване на мрежата на радиосвръзката му, организацията на засеккретените линии и „пробив" в неговите шифри.

Тази война Мартин Либицки разделя на четири съставящи – подкопаване на гражданският дух, деморализация на въоръжените сили, дезориентация на командването и война в културата.

Психологическата война предполага използването на информационните възможности и ресурси против човешкото съзнание. Ако първите три форми са традиционни и познати то „културната война", по думите на Либицки е „нещо, което Съединените щати искат да наложат на другите." Това нещо е американския начин на живот, преклонение пред американските морални и културни ценности, формиране на образ на страна достойна за подражание от всички. И на тази основа – понижаване на моралния дух на страната – противник като цяло и на нейната армия.

Тази война Мартин Либицки разделя на четири съставящи – подкопаване на гражданският дух, деморализация на въоръжените сили, дезориентация на командването и война в културата.

Хакерската война е нова форма на информационната война, зародил се заедно с появяването компютърните технологии. Нарушаване на нормалната работа на компютърните мрежи може да се извършва в мирно и военно време по отношение на информационните активи на държавата, армията и частния сектор. Основните средства, използвани за поражение са компютърните вируси, логическите бомби, чипинг-технологии. В хода на тази война могат да се нанасят мощни информационни удари по интегрираните информационни системи на противника. Информационното оръжие може да се използва за нарушаване на условията на живот (електро-, газо-, водоснабдяване), комуникационната система, движението на транспорта, финансовите операции и др. Разсъждавайки по тези въпроси М. Либицки прави следните изводи:

- за да се познават основно информационните системи на противника, трябва от мирно време да има за тях изчерпателна информация;
- за да се осигури подробна информация за информационната система на друга страна, САЩ трябва да и помогне да я създаде;
- потенциална национална стратегия на САЩ може да бъде поддържане на политика за развитие на глобалната информационната инфраструктура.

Тези изводи могат да помогнат на всеки да си обясни активността на САЩ и страните от Западна Европа за прилагане на различни форми на недържавни организации и фондове за разпространение на компютърни технологии в по-бедните държави.

Икономическата информационна война, както я определя М. Либицки е производно от съчетанието на информационната и икономическата война. Тя може да се прилага под две основни форми – информационна блокада и информационен империализъм. Разликата между тях е, че информационната блокада се води във

виртуалнята сфера чрез блокада на информационните потоци на банките, фирмите, организациите и учрежденията на страната-противник.

Информационният империализъм се изразява в завладяване на компютърните и информационните пазари и налагане на целия свят своите стандарти в тези области. „Търговията – това е война", казва този теоретик на информационните войни.

Кибер войната е информационната война на бъдещето. Тя е най-трудна за формулиране и разбиране. В нея М. Либицки включва; информационния тероризъм, семантичните атаки и „агентурната война."

Информационният тероризъм в този контекст се заключава в действия на хакери, но не насочени за разрушаване на цялата информационна система, а за използване на нейната база данни за нанасяне на удар (причиняване на загуби) на конкретен обект или субект.

Семантичните атаки по форма имат много общо с хакерските атаки. При тях информационната система на противника продължава да функционира, като външно няма промяна, но изходната информация е неадекватна на реалността.

„Агентурната война" се заключава в създаването в компютърните мрежи на виртуални „агенти", способни да изпълняват широк кръг от задачи. Тези фактически програмни роботи могат чрез придобиване на правдиви и правдоподобни данни да водят псевдопреговори (от икономически, политически и обществен характер), да генерира публикации, изказвания, коментари, да разпращат в електронните мрежи. Насочеността на тези действия са близки до психологическата война и информационния тероризъм.

Кибер войната постепенно се утвърждава като самостоятелен вид война. Следва да се отбележи, че няма утвърдена дефиниция за това, какво представлява „акт на война" в киберпространството. Министерството на отбраната на САЩ дава следното определение за целта: „Използване на компютърни мрежови операции, с цел да се възпрепятства ефективното използване на противниковите компютри, информационни системи и мрежи, като се запази боеспособността и ефективността на собствените такива". От това следва, че успехът в кибер войната ще зависи до голяма степен от това, кой може да атакува и да отбранява комуникационните и компютърни системи.

В края на 1996 г., Робърт Банкер, експерт от Пентагона, представи доклад посветен на новата програма за изграждане и бойно използване на въоръжените сили на САЩ през 21 век (концепция *„Force 21"*). В основата на концепцията е заложено разделяне на театъра на бойните действия на две основни съставящи – традиционно пространство и киберпространство, като се изтъква, че второто има по-важно значение. Р. Банкер предлага *доктрината „Киберманьовър"* да бъде естествено допълнение към традиционните военни концепции, преследва-щи целите на неутрализация и подавяне на въоръжените сили на противника. По такъв начин, сферите на водене на бойни действия освен по суша, по море, във въздуха и в космоса се допълват с т.н. *инфосфера*. Както подчертават военните експерти, основните обекти за поражение в новите войни ще бъдат информационната инфраструктура и психиката на противника.

В приетия през август 1998 г. Доктринален документ се заявява следното: „*Информационните операции се провеждат в цялото пространство от военни операции от времето на мир и през целия конфликт. Военно-въздушните сили вярват, че пълното разбиране и достигането на информационно превъзходство трябва да*

включва две концептуални области, между които съществуват тесни връзки: информацията във войната (включваща натрупването и експлоатацията на информация), и информационната война (в атакуващ и защитен аспект)".[8]

През декември 1998 г. Министерството на отбраната на САЩ въведе *„Обединена доктрина за информационните операции".*[9] Тази стъпка е наложена от необходимостта от разграничаване на понятията „информационна операция" и „информационна война" (ИВ). В документа тези понятия са формулирани по следния начин:

Информационна операция – *действия, предприемани с цел затрудняване на събирането, обработката, предаването и съхраняването на информацията от информационните системи на противника и защита на собствените информационни системи;*

Информационна война – *комплексно въздействие (съвкупност от информационни операции) върху системата за държавно и военно управление на противниковата страна, чието военно-политическо ръководство в мирно време вече е приело решения, благоприятни за страната-инициатор на конфликта, а в хода на конфликта биха довели до пълно парализиране на управленската инфраструктура на противника.*

Основната цел на ИВ е постигане на *информационно превъзходство* за осигуряване на националната военна стратегия чрез въздействие върху информационните системи на противника и същевременно укрепване на защитата на собствените информационни системи и инфраструктура.

Информационното превъзходство *се дефинира като способност да се събира, обработва и разпределя непрекъснатия поток от информация за обстановката и едновременно възпрепятстване на противника да извършва същите действия.*

Информационното превъзходство позволява получаване на интерактивна и точна картина на действията на противника и своите войски в реално време.

Съгласно ръководните документи, приети в НАТО през 1999 г., *информационните операции* се дефинират като „действия, предприемани с цел оказване на влияние върху вземането на решения в полза на собствените политически и военни цели чрез въздействие върху информацията, информационните процеси и системи за управление на противника, а също и защита на собствената информация и информационни системи". Подобно на американския подход са въведени понятията за отбранителни и настъпателни информационни операции.

Развива се и концепцията за психологическите операции (*Psyops*). Те трябва да се превърнат в сърцевината на всички бъдещи военни действия. „Военните сили на САЩ трябва да бъдат най-добре подготвени за изпълнението на психооперации за поддръжка на военните операции". Тези операции ще обхванат всички средства за масова информация – от вестниците, книгите и плакатите до „световната паяжина", музиката, комуникаторите Black Barry и персонални информационни устройства – за разпространение на черна пропаганда, позволяваща реализацията на военната стратегия на правителството. Стремежът на САЩ е да контролира целия електромагнитен спектър на Земята, което ще позволи на тези, които ще планират войни да властват над всички мобилни телефонни комуникации, PDA (personal digital

[8] „USAF Doctrine Document 2-5/August 1998"

[9] Joint Doctrine for Information Operations. Joint Publication 3-13. Washington D.C.: Joint Chiefs of Staff, Dec. 1998.

assistant – перонален цифров помощник), Web – световната „паяжина", радио, телевизионни и други форми на комуникация.

До преди няколко години, в качеството на основни източници на заплаха от киберпространството, ЦРУ посочваха само Русия и Китай. Според американските експерти, в момента, страните, планиращи и осъществяващи различни видове информационни операции, насочени срещу САЩ са повече от 20. Още повече, ЦРУ отчита, че Информационната война е заложена като неотменна част в новите военни доктрини на противостоящите на САЩ страни.

Положенията залегнали в концепцията за ИВ бяха приложени и по време на войната на НАТО против Югославия (Operation Allied Force - операция „Съюзна сила") в периода 24 март – 10 юни 1999 г. През април 1999 г. силите на НАТО са бомбардирали сръбските радио и телевизия, през май са нанесени няколко удара по телевизията в Нови сад и Прищина. В края на май 1999 г. министерството на информацията обяви, че са унищожени 17 от всичките 19 радиотелевизионни центъра във федерацията.

Доразвитите схващания за водене на ИВ се реализираха и във втората война срещу Ирак (от лятото на 2002 г. американските ВВС започват операция „Южен Фокус", която продължава до началото на март 2003 г., а от 20 март до 15 април 2003 г. продължи сухопътната операция на НАТО).

Воденето на ИВ е пряко свързано с придобиването и своевременното използване на разузнавателна информация за противниковата страна. Разузнаването е огромна и тежка машина, която се е намесила в почти всички сфери на обществения живот. Служби като ЦРУ, АНС, МИ 5, ФСБ на Руската федерация са в авангарда на борбата с тероризма и постоянно разширяват мрежата си от регионални офиси и наемат нови сътрудници. Те разполагат с огромна мощ и могат да се намесват в обществения живот по различен начин. Шпионството никога не е било толкова манипулативно и технически напреднало, колкото е днес. Разузнавачите ръководят своя собствена „държава в сянка" и имат достъп до всичките ни тайни.

През февруари 2003 г., САЩ прие *„Национална стратегия за сигурност на киберпространството"*[10], която дефинира необходимостта от координиране и концентриране усилията на всички федерални институции за защита на националното информационно пространство. В документа, наред с другите задачи, се акцентира върху необходимостта от засилване на координацията между Департамента по отбраната и националната разузнавателна общност за адекватно реагиране на киберзаплахите. Специално се подчертава, че „американското ръководство си запазва правото да реагира на евентуални кибератаки, използвайки всички средства и възможности на военния компонент на националната информационна инфраструктура."

Като продължение на този доктринален документ, през октомври 2003 беше публикувана *„Пътна карта на информационните операции"*. 11 В нея се посочва, че националната информационна инфраструктура е оперативния център на тежестта и Министерството на отбраната следва да координира усилията на федералните институции в борбата с кибератаките на противника срещу автоматизираните центрове за държавното и военно управление. Предвижда се Пентагонът да пренесе войната в

[10] The National Strategy to Secure Cyber Space. Washington D.C.: The White House, Feb. 2003.
[11] Information Operations Roadmap. Washington D.C.: U.S. Department of Defense. 30 Oct. 2003.

интернет, с цел напълно да доминира във всички световни комуникации, изпреварвайки всякакви атаки срещу САЩ и техните съюзници в тази област и за да изпревари началото на кибернетични атаки. По този начин с поставените в този документ задачи започва постепенното отработване и въвеждане на основните положения на стратегията за информационно противодействие, като част от военната доктрина и формиране на структури за управление на информационните операции.

В отделни публикации в американския и английския печат през 2006 г. се очертава схващането, че *XXI-ви век е обявен за век на Информационните войни.*

През февруари 2006 г., Обединеният комитет на началник щабовете утвърди документ, озаглавен *„Информационните операции”*[12], в който се излага визията на американското военно ръководство за тяхната подготовка и провеждане, уточняват се целите, задачите и основните принципи на информационното противоборство, както и задълженията на отделните длъжностни лица за подготовката и осъществяването на подобни операции в мирно и военно време.

В Директивата на Департамента по отбраната *D 3600.1* [13] от 14 август 2006 г., за първи път ясно дефинира основните задачи и функции на информаци-онните операции, които, като цяло, означават комплексно използване на средствата за радиоелетронна борба, операции в комуникационно-информаци-онните мрежи, психологически операции, военна дезинформация и оперативна сигурност. Информационните операции се провеждат *„с цел да се осъществи информационно въздействие, заблуждаване на противника, нарушаване работата на компютърните му системи, изкривяване на информацията, дезорганизация на базите данни и лишаване на противника от възможността да ги използва, извличане на информация от компю-търните системи и базите данни на противника, като паралелно с това се гарантира защитата на собствената информация и информационна инфраструктура”*.

Директивата разделя информационните операции на *три категории*: атакуване на компютърни мрежи (computer network attack), защита на компютърни мрежи (computer network defense), гарантиране на достъп до компютърните мрежи на противника и използването им в собствен интерес (computer network exploitation)[14].

През април 2010 г. са оповестени основните направления в реализацията на програмата за повишаване ефективността на противодействие на кибератаките срещу американските комуникационни и информационни мрежи и бази данни. Активността в тази сфера е подчинена на *„Инициативата за всеобхватна национална киберсигурност”*,[15] която се реализира под ръководството на Съвета за национална сигурност на САЩ. В нея са включени документи приети през 2008 г. като Президентската директива за осигуряване на националната сигурност № 54

[12] Information Operations. Joint Publication 3-13. Washington D.C.: Joint Chiefs of Staff, 13 Feb. 2006.

[13] Information Operations. Directive D 3600.1. Washington D.C.: U.S. Department of Defense, 14 Aug. 2006.

[14] Information Operations. Directive 10-7. Washington D.C.: U.S. Department of Air Force, 6 Sep. 2006.

[15] Butler R. Deputy Assistant Secretary of Defense for Cyber and Space Policy. Testimony before the House of Representatives Committee on Armed Services Subcommittee on Strategy Forces. Washington D.C., 21 Apr. 2010; Lynn W. Deputy Secretary of Defense. Remarks. National Space Symposium. Colorado Springs, 14 Apr. 2010.

(National Security Presidential Directive 54) и Президентската директива за осигуряване на вътрешната сигурност и безопасност № 23 (Homeland Security Presidential Directive 23).

„Инициативата" предвижда по-нататъшното усъвършенстване на мониторинга на работата на федералните комуникационно-информационни мрежи, както и реализацията на програмата „Надеждна интернет-връзка", целяща ограничаване броя на точките за включване на компютърните системи на федералните институции и учреждения към външните комуникационно-информационни мрежи, с цел своевременно да бъдат засичани случаите на нерегламентирано проникване.

„Инициативата" включва общо 12 основни направления на действията, целящи да гарантират всеобхватна защита на националното информационно пространство и фиксиране на всички опити за несанкционирано проникване.

Най-важната задача, фиксирана в „Инициативата", е защитата на базите данни от целия спектър възможни киберзаплахи. Предлага се това да стане чрез разширяване на техническите и оперативни възможности на федералните институции, отговарящи за националната сигурност. Освен това се планира да се гарантира още по-щателен контрол на каналите за доставки на най-новите информационни технологии за федералните структури, отговарящи за националната отбрана и сигурност. Предполага се, че това напълно ще изключи възможността те да бъдат снабдени с технически средства, които могат да навредят на националната сигурност.

Друго мащабно направление на вече реализираща се „Инициатива" е осъществяването на комплекс от мероприятия за качествено подобряване на системата за подготовка на специалисти в сферата на информационната сигурност. Предлага се също да се повиши ефективността на координацията на финансираните от федералния бюджет научно-изследователски и опитно-конструкторски работи в тази сфера и въвеждането на действени механизми за своевременното и преориентиране, с цел да се изключат неоправданите разходи за осъществяване на дублиращи проучвания.

Планира се разработването на стратегически подходи за ефективно противодействие на всички видове киберзаплахи. За целта се предвижда да се осъществи комплекс от мероприятия, като се започне с модернизацията на държавните структури, отговарящи за информационната сигурност, и се свърши с дефинирането на мястото и ролята на федералното правителство в този процес, така че да се гарантира непрекъснат контрол върху функциони-рането на националните комуникационно-информационни мрежи и управлението им като единен комплекс. Според експертите, това са само първите стъпки към гарантирането на сигурност в киберпространството. Всички действащи центрове за бързо реагиране на киберзаплахите трябва да бъдат обединени в една структура, което ще позволи да се контролира ситуацията в компютърните системи в режим на реално време и съществено да се повиши качеството на анализа на осъществяваните от противника кибератаки. Предлагат се мерки, насочени към създаването на структури за извършване на киберконтраразузнаване и снабдяването им с най-новите технологии за повишаване на информационната сигурност на затворените канали за свръзка и предаване на данни.

Два месеца по-късно, през май 2011 г. президентът утвърждава *„Международна стратегия за действия в киберпространството"*,[16] декларираща комплексния под-

[16] Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington. Washington D.C.: The White House, May 2011.

ход на военно-политическото ръководство на САЩ към политиката в глобалното информационно пространство. Информацията и информационната инфраструктура нато цяло са определени за стратегически ресурс. Подчертава се, че през XXI в. държавата има доста ограничена възможност за управление и контрол на киберпространството. Формиращата се полицентрична система на международните отношения все по-активна роля ще играят неправителствени структури. Това налага разширяване на международното сътрудничество в областта на информационната сигурност. Водеща роля в това направление се предоставя на Министерството на отбраната.

За първи път в официален документ е отделено особено внимание на информационното възпиране на евентуалните противници. Счита се, че структурите за колективна сигурност (като НАТО) ще съдействат за ефективното прилагане на стратегията за информационно възпиране на държавите опоненти и неправителствените структури. Важно място е отделено и на проблемите по изработване на необходимите норми на международното право в областта на информационната сигурност.

Въвежда се ново понятие в сферата на въоръжената борба – *информационно оръжие*. Под информационно оръжие, американските експерти разбират *съвкупността от специално организиран и структуриран информационен трафик, който, наред с най-новите информационни и телекомуникационни технологии, позволява целенасочено да се променя (унищожава, изкривява, блокира, копира) информацията, преодолявайки системите за защита, да се ограничава достъпа на законните ползватели, да се осъществява дезинформация, да се нарушава функционирането на носителите на информация и да се дезорганизира работата на техническите средства, компютърните системи и информационно-комуникационните мрежи на противника* [17].

С други думи в информационното оръжие се включва целия арсенал от средства за несанксиониран достъп до информацията и извеждането от строя на електронните системи за управление на противника. Чрез средствата за психологическо въздействие се цели да се причинят не поражения на здравето на хората, а да се доведат до блокиране на неосъзнато ниво на свобода за волеизлияние на човека, загуба на способност за политическа, културна и личностна самоидентификация, манипулация на общественото съзнание и дори разрушаването на информационното и духовното пространство.

С това принципно се променят механизмите за ескалация на военните конфликти, защото макар и ограничено използване на информационно оръжие по обектите от военната или гражданската инфраструктура може да завърши с конфликт още на ранен стадий, преди началото на активни бойни действия. Владеенето на такова оръжие осигурява политическо и военно-стратегическо преимущество. Подобно на ядреното оръжие, информационното може да се използва за политически натиск и за възпиране на потенциалния агресор. Ефективността на такъв вид заплаха се определя от нивото на технологичната база на информационната система на държавата.

Постановките на тази стратегия се развиха в доктриналния документ на МО от юли 2011 г. *„Стратегия на Министерството на отбраната за операциите в кибер-*

[17] Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington. Washington D.C.: The White House, May 2011.

пространството".[18] При нейното представяне в Университета за национална отбрана заместник-министъра на отбраната Уинлям Лин заяви: „САЩ си запазва правото, в съответствие със законите на войната да отговори на кибератаките пропорционално и по справедлив начин в същото време и на същото място, както ние изберем".

Документа определя пет стратегически инициативи, с изпълнението на които МО може да защити националната инфраструктура:

1. Признаването на киберпространството за приоритетна сфера за оперативна дейност;

2. Прилагане на „активна защита" на комуникационно-информационните мрежи и компютърни системи;

3. Ефективно взаимодействие на Министерството на отбраната с другите федерални ведомства и частни компании за осигуряване на информационната сигурност.

4. Установяване на активно сътрудничество със съюзниците и партньорите в областта на колективната защита от киберзаплахи;

5. Увеличаване на финансовите и материалните ресурси, влагани за развитието на научно-техническата база на киберзащитата, подготовка на висококвалифицирани профилирани специалисти.

От направения кратък обзор на доктриналните документи следва извода, че САЩ декларират необходимостта от надежден, отговарящ на съвременните изисквания национален потенциал за водене на информационно противоборство. Нарастващата роля на информационното оръжие, като важен елемент за водене на войните от ново поколение, води до нарастване на зависимостта и ефективността на бойните действия от иновационните цифрови технологии. Това неизбежно довежда до ръст на уязвимостите на цялата национална информационна инфраструктура и я превръща в приоритетна военна цел за противника.

Принципния извод от всички документи определя необходимостта от надеждна и всеобхватна защита на информационното пространство и на цялата информационна инфраструктура.

2. Новите измерения на информационната война

В международен план в началото на XXI в. се оформят три центъра, в които най-активно се развиват стратегиите и силите за информационна война – САЩ, Русия и Китай.

В първия световен център – САЩ, в качество на технологичен инструментариум при използването на информационното оръжие се използва *„Глобалната информационна мрежа"* (Global Information Grid), която е развърната в интерес на МО на САЩ и свързаните с него разузнавателни структури за осигуряване на достъпа до единните разузнавателни ресурси на всички военни бази, командни структури, бойни платформи и пунктове с временна дислокация.[19] За тази цел се извършва постепенно преустройване на съществуващата *„Глобална система за оперативно управление"* (Global Command and Control System), под ръководството на Агенцията по информационните системи на Министерството на отбраната (Defense Information Systems Agency).

[18] Department of Defense Strategy for Operating in Cyberspace. Washington D.C.: U.S. Department of Defense, July 2011.

[19] Libicki M. Who Runs What in the Global Information Grid: Ways to Share Local and Global Responsibility. Santa Monica: RAND, 2000.

Основното техническо средство за водене на информационната война е Глобалната система за радиоелектронно разузнаване *„Ешелон”* (ECHELON), която има възможност да прихваща информация, предавана по електронните комуникационни канали и да прослушва телефонните разговори във всяка точка на планетата, чрез контрол на радиоефира и кабелните линии.[20]

В доклад на Комитета за граждански права към Европейския парламент от 1997 г. се твърди, че съществува огромна система за електронен шпионаж, която контролира ежедневно всички комуникации в Европа – всеки разговор, всеки факс, всяко електронно писмо. Обменяните съобщения се четат от компютри, които прилагат свръхнови технологии и изкуствен интелект за разчитане на съдържанието им. Имената и данните за комуникиращите се предават на оператори, които преценяват дали е необходим допълнителен анализ на данните на хората.

Тази инсталация е монтирана в *13-та полева станция* USASA, разположена в *базата „Менуит Хил”* (*Menwith Hill*) в Северен Йоркшир на Кралските ВВС, използвана „под наем” от 1996 г. от Вашингтон и Белия дом – фиг. 2. Станцията е „под шапката” на Агенцията за национална сигурност (АНС) (*National Security Agency – NSA*) и се ръководи от генерал–лейтенант Кийт Алекзандър. Ръководството и отговаря само пред президента на САЩ и неговите съветници по национална сигурност. Има възможност да подслушват всеки сигнал и разговор, проведен в Европа, Северна Африка и Западна Азия. Базата постепенно се разраства, а нейната важност проличава от факта, че АНС затвори други свои наблюдателни станции на Острова. Новото й официално название е – *„Регионален оперативен център за сигнално разузнаване”*, който отговаря за управлението на обектите за дистанционно автоматизирано събиране на разузнавателни данни – само подчертава стратегическото значение на базата. С инсталираната апаратура могат да се прехванат, анализират и обработят и автоматично да се препратят в САЩ всички сигнали преминаващи по кабел, чрез микровълнови радиоточки или сателити.

В интерес на системата „Ешелон” работят технически средства на съюзниците и партньорите на САЩ (Великобритания, Канада, Австралия и Нова Зеландия), които следят радиоефира в техните географски региони. Системата се състои от: 1. Орбитална сателитна групировка за следене, която контролира огромно количество електронни комуникационни средства; 2. Суперкомпютри, способни да анализират до 10 мирд. съобщения в денонощие; 3. Пунктове за прехват, развърнати в целия свят (в американски военни бази, и на места прикрити като граждански организации), които прехващат, записват и декодират съобщенията.

Разкритията на бившия сътрудник на ЦРУ Едуард Сноудън от май 2013 г. потвърждават, че съществуват федерални програми за следене на телефонни и интернет комуникации. Чрез пряк достъп до сървърите на девет американски интернет гиганта, сред които „Майкрософт”, „Яху”, „Гугъл” и „Фейсбук”, АНС и ФБР следят дейността на чуждестранни граждани. С въведената през 2007 г. тайната програма с кодово име *„Призма” (PRISM)* АНС може да се логва в сървърите на компаниите през специален портал, за да събира информация за потребители, за които има „разумни доводи” да се смята, че са чужденци. Според директора на АНС ген. Кийт Алегзандър, програмата е била прекратена през 2011 г., защото АНС преценила, че не била ефикасна за предотвратяване на терористични заговори.

[20] Hildreth S. Cyber Warfare: Background and Issues for Congress. Congressional Research Service (CRS) Report for Congress. RL 30735. Washington D.C.: CRS, 19 June 2001.

Фиг. 2. Външен изглед на базата „Менуит Хил" в Северен Йоркшир – Англия

Публикациите в световните информационни средства показват друго лице на САЩ при воденето на кибервойната. Интернет изданието „И Ю обзървър"[21], като се позова на съобщение на руската лаборатория за компютърна сигурност „Касперски лаб.", през януари 2013 г. изнесе информация, че неизвестни хакери в продължение на пет години са крали кодирани файлове на ЕС и НАТО. При операцията, наричана „Червения октомври", са били откраднати по електронен път документи от посолства и правителствени и военни институции на 16 от 27-те страни от ЕС - Австрия, Белгия, България, Чехия, Кипър, Финландия, Германия, Гърция, Ирландия, Италия, Латвия, Литва, Люксембург, Португалия, Словакия и Испания. Засегнати са дипломатически и правителствени компютърни мрежи в Австралия, Иран, Израел, Русия и САЩ. Според „Касперски лаб." този списък не изчерпва жертвите на „Червения октомври".

В Белгия, където се намират централите на ЕС и НАТО, са регистрирани 15 отделни незаконни проникванията в компютърни мрежи. През последните пет години хакерите имали възможност да следят натиснатите клавиши на клавиатурата и списъци на посещавани уебсайтове. Откраднати са списъци с адреси и телефони, история на разговорите и изпратени и получени есемеси от айфони и смартфони „Нокиа", както и устройства, работещи под Windows Mobile. Германското списание „Шпигел" на 3 февруари 2014 г. изнесе информация, че са откраднати имейли и пароли на служители от всички министерства, както и на депутати; всички жертви на атаката са около 16 млн. души и лични данни на 2 млн. абонати на мобилния оператор „Водафон".

Европейски лидери реагираха остро на твърденията на германско списание, че САЩ водят широкомащабна програма за подслушване на дипломатически офиси и компютърни мрежи на ЕС, като някои от тях заявиха, че са очаквали подобно следене от врагове, но не и от най-близкия си икономически партньор, пише в. „Вашингтон пост".

[21] EUObserver.com

Според Е. Сноудън „АНС се цели в информацията на всички. Събира я, филтрира я, анализира я, съхранява я за известно време - просто защото това е най-простият и най-ефикасният начин да постигне целите си. Макар че може да искат да подслушват само някой чуждестранен агент или някой заподозрян в тероризъм, те събират вашата информация... Всеки анализатор по всяко време може да подслушва всекиго - зависи от властта, която му е дадена". Това е поредното потвърждение, че АНС от години чрез поредната програма за масово следене, е събирала масиви от данни за имейли и интернет трафик и на американски граждани.

Този процес продължава. Потвърждение на това е публикацията в британския вестник „Гардиън" (The Guardian) от 13 май 2014 г.: „Агенцията за национална сигурност на САЩ тайно поставя „бръмбари" в маршрутизатори, сървъри и друго мрежово оборудване, което доставя в други страни. По този начин електронното разузнаване може да следи цели сегменти от интернет." Тези сведения се съдържат в новата книга на бившия журналист на изданието Глен Гринвалд: „Секретните операции се състоят в това, че АНС получава или прихваща партиди с оборудване, което е подготвено за износ, след което инсталира тайни средства за наблюдение, отново опакова стоката с заводски печати и след това я изпраща на крайния получател. В крайна сметка, устройството установява връзка с АНС", констатира Гринвелд на страниците на изданието.[22]

Схващането на английското министерство на отбрана, изразено от министъра Ник Харви пред вестник „Гардиан" на 31 май 2011 г., е следното: „кибероръжията са неразделна част от въоръжението на държавата" и „действията в киберпространството ще формират част от бойното поле в бъдеще" в свят, където дигиталната инфраструктура става все по-широка. „Последствията от една добре планирана, добре изпълнена атака срещу нашата дигитална инфраструктура може да бъдат катастрофални. При ядрените или биологичните оръжия техническият праг е висок. В киберпространството пръстът, кръжащ над бутона може да е всеки от държава до студент", посочи министърът.

Отчитайки важността на защитата на компютърните мрежи и действия в киберпространството, през последните 5 години водещите държави усилено изграждат управленски структури и специализирани командвания за киберзащита.

В състава на ВВС на САЩ от септември 2007 г. се сформира временно ново командване, което да отговаря за „*войната в киберпространството*".[23] Разположено е във военно-въздушната база в Барксдейл, щата Луизиана, от където се провеждат всички операции на американските ВВС във виртуалното пространство. На базата на това временното виртуално командване постепенно "*ще бъде създадено пълно Киберкомандване на ВВС на САЩ*", където "*ще се създават, тренират и снабдяват части за провеждане на продължителни глобални операции в киберпространството и посредством киберпростран-ството, които ще бъдат напълно интегрирани с въздушните и космически операции*". Създаването на временното Киберкомандване става след нарасналата заплаха от „*опасни хакерски атаки против западните държави от територията на Китай*", а също и след нападението на хакери на естонски правителствени сайтове през май 2007 г.

[22] The Guardian: Агенцията за национална сигурност на САЩ поставя „бръмбари" в маршрутизаторите и сървърите, които изнася зад граница, 31 май 2014 г., Агенция "Фокус". http://www.focus-news.net/news/.

[23] http://www.factor-news.net/index_.php?cm=3&id=12400

С Указ, подписан от министъра на отбраната на САЩ Робърт Гейтсъм през юни 2009 г., САЩ създадоха ***Киберкомандване*** (*U.S. Cyber Command*), което е базирано във Форт Мид, щат Мериленд – фиг. 3. Силите на новия щаб отговарят за защитата на американските военни системи, но не и на други правителствени или частни мрежи. Министерството на отбраната на САЩ използва около 15 000 електронни мрежи и използва около 7 милиона компютри и други технологични устройства. Командването от май 2010 г. е подчинено на АНС, която се ръководи от генерал-лейтенант Кийт Алигзандър. То се фокусира върху защитата и поддръжката на мрежите на Министерство на отбраната и консолидира съществуващите опити на Пентагона да защити своите мрежи и да действа в киберпространството. Тези усилия до тези момент се контролират от Стратегическото командване на САЩ в Небраска. При създаването в състава на командването са включени около стотина души и е подсигурено с ресурс от 120 млн. долара.

Формираното Киберкомандване е на стратегическо ниво и му се възлагат следните задачи:

1. Управление на рисковете в кибернетичното пространство чрез усъвършенстване на подготовката и информираността и подобряване на условията за сигурни и гъвкави мрежи.

2. Осигуряване на достъп и ефективност на мрежите чрез създаване на партньорски връзки, система за колективна отбрана и поддържане на общо работно пространство.

3. Осигуряване на условия за развитие на интегрирани способности чрез тясно сътрудничество между командванията на войските, службите, агенциите и специалистите, които да способстват бързото създаване и внедряване на иновации, отнасящи се до кибернетичното пространство.

Фиг. 3. Зала от Киберкомандването на САЩ

От юни 2011 г. е решено щата на Киберкомандването да бъде увеличено от 900 на 4900 служители – както военни, така и цивилни. Предвижда се в негово подчинение да се създадени три типа сили: 1. Сили за защита на компютърните системи (електрически мрежи и друг тип инфраструктура на САЩ); 2. Сили за

нападателни операции на американската армия в чужбина; 3. Сили за защита на вътрешните мрежи на Пентагона.

По информация, изнесена във в. „Ню Йорк таймс" по поръчка на президента Барак Обама, Пентагона е разработил секретен доклад, на базата на който ще бъде направена корекция в стратегията за отбрана на страната. Ще се промени категоризирането на вражеските актове на хакерските атаки по интернет, застрашаващи националната сигурност на САЩ – срещу ядрените реактори на страната, петролопроводите, газопроводите и транспортната система. Като повод за това е „масираното кибернападение" на 21 май 2011 г. срещу „Локхийд Мартин" – най-големия подизпълнител на договори за въоръжаване на американската армия. Докладът предвижда три вида отговор – президентът да може да налага икономически санкции на бизнес субекти или на цели държави, да заповядва контраатаки в киберпространството или направо военен удар.

Друга публикация във в. „Вашингтон пост" се изнася информация, че кибероръжията на САЩ са описани в свръхсекретен списък, до който има достъп американската разузнавателна общност. В по-голямата си част те представляват свръхсложни вируси за саботаж на противниковите системи. Използването им може да става само с изрична президентска заповед.

Вторият световен център на силите за информационна война е Русия. В него в края на 2011 г. Министерството на отбрана на Руската федерация прие собствена стратегия за водене на война в киберпространството: *„Концептуални възгледи за дейността на Въоръжените сили на Руската федерация в информационното пространство"*. В този стратегически документ са разработени правилата свързани с използването на информационните ресурси за решаване на задачите по отбраната и сигурността. Те включват: ефективно съдържание за предотвратяване и разширяване на военните конфликти в информационното пространство, което ще се реализира с мирни средства – преговори, съглашения при тясното сътрудничество със Съвета за сигурност на ООН или на други регионални органи.

От март 2012 г. Русия взе решение за създаване на Киберкомандване във въоръжените сили, което ще осигурява информационна безопасност на руската армия и на цялата инфраструктура на държава – фиг. 4. То ще се грижи за защитата на комуникационните и информационните активи на ВС на Русия и на критичната инфраструктура на държавния и частния сектор от заплахи в киберпространството.[24]

Планира се Киберкомандването да се създаде до края на 2014 г. с ранг на нов род войски както Въздушно-десантните и Ракетните войски със стратегическо назначение. На първия етап от развитието на командването, то функционира като главно управление в Министерството на отбраната и действа в състава на Войските за въздушно-космическа отбрана. По думите на началника на 8-мо управление на ГЩ на Въоръжените сили на Руската федерация Юрий Кузнецов, се разчита специалната структура за осигуряване на защита на военните обекти от различни външни атаки поетапно да бъде напълно развърнато до началото на 2017 г.[25]

През 2013 г. президента на Русия Владимир Путин подписва указ *„За създаване на държавна система за откриване, предупреждаване и ликвидиране на пос-*

[24]http://telegraf.com.ua/rossiya-i-sng/809659-cherez-god-v-armii-rossii-poyavitsya-kiberkomandovanie.html

[25] http://rus.ruvr.ru/2014_02_02/Minoboroni-formiruet-cifrovuju-zashhitu-5309
http://eurasian-defence.ru/node/26569

ледствията от компютърни атаки за информационните ресурси на Руската федерация". Предвижда се тази система да стане една от структурите на Федералната служба за сигурност (ФСБ). Към август 2013 г. в Русия съществуват няколко органа за противодействие на виртуални заплахи: в Министерството на вътрешните работи това е *Управление „К"*, а към ФСБ – *Център за информационна безопасност*. Дейността на тези две структури не се пресичат с дейността на третата силова киберструктура.

Фиг. 4. Зала от Киберкомандването на Русия

Управление „К" извършва разследвания на компютърните престъпления на територията на Руската федерация и привлича злоумишлениците към отговорност. Центърът за информационна безопасност противодейства на чуждите специални служби във виртуалното пространство, на екстремистки организации и криминални структури, застрашаващи националната и икономическата сигурност на Русия. Киберкомандването на МО ще възпира киберзаплахите при опити на открити посегателства на интересите на страната от страна на другите държави.[26]

В отговор на *„Международна стратегия за деистви в киберпространството"* на САЩ, през юли 2011 г. президента на Русия подписва *„Основи на държавната политика на Руската федерация в областта на международ-ната информационна безопасност за периода до 2020 година"*.[27]

Отчитайки необходимостта от снижаване рисковете и конфликтите в киберпространството, през юни 2013 г. на срещата на „Голямата осморка" в Северна Ирландия, САЩ и Русия подписаха споразумение за сътрудничество по въпросите на борбата с тероризма и оръжията за масово унищожение. В него се предвижда поддържане на постояннодействаща свръзка, работеща в режим на реално време за взаимно оповестяване за инциденти, създаващи заплахи за националната сигурност.[28]

[26] http://hitech.newsru.com/article/20aug2013/kiberugroz
[27] http://warfiles.ru/show-36901-nuzhno-li-rossii-kiberkomandovanie.html
[28] http://inosmi.ru/russia/20130618/210145773.html#ixzz325W4lnf3

В третия световен център Китай - през юли 2010 г. във Въоръжените сили на Китайската народна република е създадено „*Управление по въпросите на информацинната сигурност"*, което е пряко подчинено на Генералния щаб и в този смисъл е аналог на Киберкомандването на САЩ и Русия.

В Китай е разработена *„Концепция за Информационна война"*. Паралелно с националните представи се изучава и въпросът за създаването на формирования за информационна война - специални военни подразделения, състоящи се от високо класни компютърни експерти, подготвяни в най-добрите китайски университети, академии и учебни центрове. Полагат се големи усилия за привличането на млади и талантливи специалисти. При подготовката на въоръжените сили особено внимание се отделя на въпросите, свързани с информационната война.

Според схващанията за ИВ, тя трябва да се води на три нива: *I ниво* – високо квалифицирани кибер-войници от армията, които ще осъществяват кибератаки по чужди компютърни мрежи и киберотбраната на своите мрежи в началото на бойните действия (при обявяване на войната); *II ниво* – групи от граждански лица или военизирани специалисти по водене на кибервойна от държавни органи и институти и частни корпорации, които ще бъдат мобили-зирани в *Киберармията на Китайската народоосвободителна армия* в началото на кибервойната. В мирно време провеждат постоянни „разузнавателни" атаки по компютърните мрежи на правителствените и бизнес структури на противниците на Китай; *III ниво* – армия на „хакерите – патриоти", които осъществяват киберата-ки по информационните мрежи на другите страни. Китай активно развива космическите си програми и вече е изстрелял ракети, способни да свалят други ракети. Разработил е специални средства за създаване на смущения и блокиране на информационни потоци. Разпространявал е и специални вируси за борба с активната отбрана, които са съставни части на информационната война.

Своите схващания и сили за водене на информационна война развиват и други водещи световни военни сили.

Във Великобритания с проблемите на информационната война се занимава *Департаментът по правителствени комуникации* (The Government Communication Headquarters), за който работят 6000 специалисти. Схващанията на британските военни специалисти са аналогични на тези на американските. Във връзка с това, се използва юридически нормативен акт *„Регламент за разследващи пълномощия"* (Regulation of Investigatory Powers Act) от 2000 г., който е приложим в значителна степен за действия в киберпространството. Съгласно този документ, нападението върху една информационна система се счита за углавно престъпление с всичките произтичащи от това последствия. Освен това, този акт дава основание на британските правителствени служби да прихващат и четат електронна поща, а също и да разшифроват лични файлове.

От февруари 2009 г. Германското военно министерство в казармата в Рейнбах, близо до Бон, сформира специална група за водене на кибервойна. Задачата на хакерите в униформа са да „проникват, манипулират и унищожават вражески мрежи". На негова база е създаден *Център за осигуряване на безопасността на информационната техника* (Bundesamt fur Sicherheit in der Informationstechnik) с щат около 500 сътрудници и годишен бюджет от около 50 млн. евро. В общи линии, представата на немските специалисти за информационната война не се различава съществено от американските и също включва отбранителни и настъпателни информационни опе-

рации. Същевре-менно се наблюдава тенденция за по-задълбочена систематизация. За разлика от американските експерти, немските разглеждат управлението на средствата за масова информация като елемент от информационната война. Освен това, те отделно разглеждат икономическата информационна война, тъй като е извършена оценка на размерите на евентуалната вреда, която може да бъде нанесена върху немския бизнес и икономика чрез информационни диверсии.

Френските експерти се придържат към концепцията за информационна война, състояща се от два основни елемента: военен и икономически. Военната съставяща предполага сравнително ограничена роля на информационните операции, тъй като ИВ се разглежда в контекста на конфликти с малка интензивност и миротворчески операции. При този подход се предполага, че съюзниците не могат да бъдат противници. Икономическата или гражданската концепция включва по-широк спектър на използване на информационните операции. Гледната точка на френските експерти се отличава с по-дълбоко изучаване на конфликтите в икономическата сфера и в подобни ситуации те не се чувстват свързани с рамките на НАТО, ООН или мнението на САЩ. Техният подход към икономическия конфликт допуска, че страната-съюзник може да бъде и обект на Информационната война

През 2010 г. Министерството на отбраната на Израел създаде *Подразделение за борба с кибертероризма и провеждане на специални операции в Глобалната мрежа, информационните мрежи на правител-ствените, финансовите и силовите структури на потенциалния противник*. То е радиоразузнавателно формирование подчинено на Разузнавателно управление на Генералния щаб на Националните въоръжени сили на Израел.

В края на януари 2013 г. в Генералния щаб на Турция се създаде *Киберкомандване за осигуряване на безопасността на националната инфраструктура и противодействия на кибернападение*. За целта са усилени възможностите за защита на киберпространството и е прието решение за създаване на *Управление по киберотбрана*, което ще действа в координация с министерството на транспорта, мореплаването и комуникациите на Турция и с други национални институти. Това управление ще бъде в тясно сътрудничество с НАТО. Идентични структури са развърнати във ВС на Франция, Индия, Австралия и др.

В началото на февруари 2014 г. ИТАР-ТАСС съобщи, че в отговор на засилващите се заплахи за киберсигурността й, Япония е сформирала във въоръжените си сили първото *Специално подразделение за компютърна защита*.[29] То вече е участвало в секретно учение, съвместно с Пентагона. До сега за защитата на компютърните мрежи във въоръжените сили на страната са се грижили специалисти към отделните щабове. Новото спецзвено обединява програмисти и хардуеристи от военната сфера, които ще контролират всички държавни компютърни системи. Предвижда се звеното да прерасне в Правителствен център за кибернетична сигурност.

От 2010 г. Австралия и Индия също активно развиват схващанията и силите си за кибер защита.

В средата на 2010 г. правителството на Индия прие решение за създаване на *Управление за шпионаж в компютърните системи на страните-противници*, което да е включено в състава на специал-ните сили на страната. Създаде се *Национална база данни за сигурност,* в която се регистрират потенциалните защитници

[29] http://www.manager.bg/

на индий-ското киберпространство. Планира се на нейна основа да се създаде *Индийска киберармия*, чийто състав да включва програмисти и експерти-хакери.

През януари 2010 г. в Министерството на отбрана на Австралия е открит *Център за киберсигурността на МО*, който е подразделение на *Управлението за свръзки на МО*. От началото на 2011 г. в изпълнение на Националната стратегия за киберсигурност е създаден *Национален орган за киберсигурност*, който е структура на Австралийското разузнаване. Предвижда се в този орган да взаимодейства с *Националното киберподразделение*, което ще осигурява киберзащитата на правителствените и военни информационни мрежи, на комуникационните и информационните ресурси на важни инфраструктури от кибератаки.

Направеният анализ показва, че развитието на концепциите за водене на информационните войни на национално ниво е предоставено предимно на научните институти и академии на военните ведомства, а органите за защита са с ранг на вид въоръжени сили на МО или са управления от състава на разузнавателните управления на генералните им щабове.

Въпросите свързани с разследването на компютърните престъпления и противодействието на лица и организации застрашаващи националната сигурност са приоритет на структури на Министерството на вътрешните работи или на специализирани административни структури.

3. Киберсигурността в Обединена Европа

Развитието на компютърните технологии и глобализацията на световното информационно пространство винаги е стояло в центъра на вниманието на европейските органи за сигурност. През последните три-четири години вследствие на нарасналите заплахи от терористични атаки, както и на бурния ръст на световната киберпрестъпност, фокусът на усилията както в световен, така и в европейски мащаб се насочи към т.н. „защита на критичната информационна инфраструктура". След *„Директивата за идентификация и оценка на защитата на европейската критична инфраструктура"* от 2006 г. Европейската комисия издаде през март 2009 г. *„Комюнике относно защитата на критичната информационна инфраструктура"*.

Редица документи на Европейската комисия определят мрежовата и сигурност като един от най-важните фактори за изграждането на „единното европейско информационно пространство". Поради това, на европейско ниво се предприемат редица конкретни действия в това направление, включително създаване през март 2004 г. на *Европейска агенция за мрежова и информационна сигурност* (ENISA). Нейната основна цел е да способства за подобряване на мрежовата и информационната сигурност в Европейския съюз и да допринесе за непрекъсваемостта на бизнеса и безпроблемното функциониране на вътрешния европейски пазар.

ENISA подпомага Комисията, държавите-членки, а оттам и бизнеса в изпълнение на изискванията на мрежовата и информационна сигурност, включително и настоящото и бъдещото законодателство на Европейския съвет. ENISA се стреми да служи като център за експертни знания за държавите-членки и институциите на ЕС, които да търсят съвети по въпроси, свързани с мрежовата и информационна сигурност.

Въведените Рамкова директива за електронните комуникации (чл. 13а и 13б от Директива 2002/21/ЕО), Директива 95/46/ЕО (чл. 17) и Директива 2002/58/ЕО (чл. 4) изискват доставчиците на електронни услуги и администраторите на лични данни да предприемат адекватно управление на рисковете в своите мрежи и защита

на данните в обществените мрежи и да докладват на компетентните държавни органи при инциденти.

В резултат на дългогодишна работа на специалистите по киберсигурност, на 7 февруари 2013 г. бе приета *„Стратегия на ЕС за киберсигурност – отворено, безопасно и сигурно киберпространство"* от Европейския парламент, от Съвета на Европа, от Европейските комитети за икономика, социални въпроси и за регионите.

Целта на стратегията е защитата на фундаменталните права на гражданите, свобода на изразяването, защита на личните данни и частния живот и осигуряване на достъп до информация. Демократично и ефективно управление на мрежите от многото оператори и споделяне на отговорността за осигуряване на сигурността.

Представени са основните принципи на киберсигурността:

1. Основните ценности на ЕС важат в еднаква степен в цифровия и физическия свят.

2. защита на основните права, свободата на изразяване на мнение, личните данни и неприкосновеността на личния живот.

3. Достъп за всички.

4. Декократично и ефикасно управление с участието на множество заинтересовани страни.

5. Споделена отговорност за гарантирането на сигурността.

Целта на Стратегията може да се реализира чрез разработване на общи минимални изисквания за мрежова и информационна сигурност. Всяка страна трябва да изгради: национални компетентни органи за Мрежова и информационна сигурност (МИС), да създаде функционираща отговорна структура за справяне с критични компютърни ситуации (Computer Emergency Response Team – CERT), да разработи и приеме национална стратегия и координационен план за МИС, да изгради координация с органа на Европейския съвет - CERT-EU.

В стратегията е представена визията на ЕС за кибернетична сигурност по отношение на пет приоритета:

• Постигане на устойчивост в киберпространство;

• Чувствително намаляване на киберпрестъпността;

• Разработване на политика за киберотбрана и способности, свързани с общата политика за сигурност и отбрана (ОПСО);

• Разработване на промишлени и технологични ресурси за киберсигурност;

• Създаване на съгласувана международна политика на Европейския съюз за киберпространството и насърчаване на основните ценности на ЕС.

За подобряване на координацията в това направление ЕС ще разчита на базирания в Хага „Център за борба с киберпрестъпността" (European Cybercrime Center (EC3)), открит на 11 януари 2013 г.

В Р. България със „Закона за електронното управление" еднозначно се определи държавния орган, отговорен за мрежовата и информационна сигурност в администрацията - Министерството на транспорта, информационните технологии и съобщенията, при това, във всичките аспекти на тази отговорност:

- разработване на политики и нормативни актове;
- разработване и поддържане на инструменти за реализация на политиките;
- контролни функции.

В изпълнение на изискванията на закона:

➢ с *„Наредбата за общите изисквания за оперативна съвместимост"* и нейните 13 приложения беше формулирана държавната политика в областта на мрежовата и информационна сигурност;

➢ беше създаден с помощта на ENISA *Правителствен център за действие при инциденти в компютърната сигурност* (*Gov-CSIRT*), който е акредитиран от компетентния европейски орган Trusted Introducer*;*

➢ беше приета *„Методология за планов и текущ контрол на информационната сигурност",* както и създаден административен капацитет за нейната реализация.

От 2011 г. функционира *Правителствен център за реагиране срещу компютърни инциденти CERT - България* (Bulgarian Computer Security Incidents Response Team - CERT Bulgaria). Разработени са съвременни процедури за съхранение на особено чувствителна инфор-мация в съответствие с изискванията за оперативна съвмести-мост и информационна сигурност. Целта е гражданското обществото да получи солидни гаранции, че тези инфраструктури са устойчиви на бедствия, кибератаки и други кризисни ситуации.

Мисията на центъра е да подпомага ползвателите на услугите му в извършването на проактивни дейности за намаляване рисковете от инциденти в компютърната сигурност на мрежите за обмен на некласифицирана информация и да асистира при разрешаването на такива инциденти в случай, че вече са възникнали. Центърът предоставя централизирана база данни с информация, свързана с осигуряване на сигурна и защитена информационна среда. Целите, които се поставят включват:

- защита на информацията и технологичните активи;
- ограничаване директното влияние на инцидентите в сигурността върху информационното общество;
- помощ при възстановяване от инциденти;
- оценяване на въздействието от инциденти в сигурността;
- събиране и разпространение на техническа информация, свър-зана с инциденти в компютърната сигурност, както и с уязвимости в сигурността на системите и начините за предотвратяването им;
- провеждане на изследвания, свързани с нови технологии в мрежовата и информационна сигурност;
- провеждане на обучения, свързани с информационна сигурност и управлението на инциденти.

След проведени трансформации на Правителствения център, към момента е в структурата на Изпълнителна агенция електронни съобщителни мрежи и информационни системи (ИА ЕСМИС), на Министерството на транспорта и информационните технологии и съобщенията, където е сформирана *Дирекция „Център за реакция при инциденти във връзка с информационната сигурност"* (GovCERT.bg).[30]

Специалистите от центъра активно си сътрудничат с ENISA и вземат участие в организираните учения по киберзащита. През април 2014 г. в нашата страна се

[30] Постановление № 69 от 2 април 2012 г. за изменение и допълнение на Устройствения правилник на Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи", Обн.ДВ. бр. 28 от 6 април 2012 г.

проведе учение *Cyber Europe 2014* (CE2014), в което участваха 200 организации и над 400 експерти по кибер сигурност от Европа.

В Р. България за извършване на дейности по защита на националната сигурност от посегателства, насочени срещу независимостта и суверинитета, териториалната цялост, националните интереси, установения конституционен ред и основните права и свободи на гражданите е упълномощена Държавна агенция „Национална сигурност" (ДАНС). Към нея има обособена специализирана дирекция „Технически операции",[31] която изпълнява една от задачите на агенцията по защита от „компютърни престъпления, извършени във или чрез компютърни мрежи и системи".

На третия регионален форум по киберсигурност и киберсигурност за държавите от Югоизточна Европа, проведен е София на 11 и 12 ноември 2013 г., началника на кабинета на министъра на отбраната Иван Жерков обяви, проблемите на киберсигурността са приоритетни направления в работата на българското Министерство на отбраната и че от началото на 2014 г. стартира проект на МО за изграждане на способности за кибер защита. Проектът е включен в инвестиционната план-програма на Министерството до 2020 г. [32] За реализирането му трябва да се предприемат адекватни мерки на политическо и военно-технологично ниво.

На политическо ниво се налага определяне на отговорности за всички страничленки на НАТО в областта на информационната сигурност, което се изразява в ускоряване на процеса по изграждане на способности за защита на критичната комуникационна и информационна инфраструктура на държавата.

На военно-технологично ниве се налага разработване и внедряване на нови посъвърженни и устойчиви методи и средства за защита и гарантиране на информационната сигурност като цяло.

Реализирането на проекта предполага привличането не само на специалисти от административните структури на държавта, но и на научни работници от ВУЗ и БАН, работещи по проблемите на информационната сигурност. Единственото научно звено в България, което е специализирано в областта на компютърната вирусология, компютърна и комуникационна сигурност е Националната лаборатория по компютърна вирусология на БАН.

На национално ниво все още няма разработена и приета Стратегия за киберсигурност. Очаква се в близко бъдеще сформираната междуведомствена работна група да предложи стратегия, състав, правомощия, мисия, функции и задачи на Национален орган по кибернетична сигурност, както и да подготви проект на Решение на Министерски съвет за неговото ситуиране.

4. Води ли се необявена кибервойна?

Този въпрос основателно се поставя от доста време. Съдейки по публикациите в печатните и електронните световни медии може да се извода, че повече от седем години се води необявена кибервойна.. Хакерските атаки се превърнаха в инструмент на международната политическа борба.

През април 2007 г. на фона на безредиците в Талин, свързани с премахването на паметника на Бронзовия войник, започнаха кибератаки на сайта на правителството на Естония и на други държавни учреждения. Министъра на външните работи обвини за

[31] Закон за Държавна агенция „Национална сигурност", Обн. ДВ брой 109, 20.12.2007 г., изм. ДВ брой 65, 23.07.2013 г.

[32] http://temadaily.bg/publication/14780/

тези атаки Русия и предложи ЕС да въведе санкции, но тези обвинения не бяха доказани. В отговор на това в Талин се разкри *център на НАТО по киберзащита.* От 1-ви февруари 2014 г. Естиния предостави лабораторията си по киберотбрана на НАТО, за да могат експертите от Алианса да развиват своята киберзащита и използват силите си с максимална ефективност – фиг. 5.

Фиг. 5. Общ изглед на Центъра на НАТО по киберзащита

По време на „петдневната война" (8 – 12 август 2008 г.), операцията на руската армия при агресията на Грузия в Южна Осетия се извършиха множество хакерски атаки. Тези атаки целят лишаване от достъп до услуга – атакуват се Web-сървъри, за да станат недостъпни за Интернет.

На 1 декември 2008 г. в. „Лос Анджелис таймс" съобщи, че руски хакери са направили пробив в системата на Пентагона. Електронната защита на Министерство на отбраната на САЩ е била заобиколена от компютърен вирус, дело на руски хакери.

В началото на 2009 г. пакистански хакери атакуват важни обекти от индийската инфраструктура, държавната банка на Индия и други финансови учреждения. Атаките са проведени в отговор на исканията властите на Индия да унищожи всички терористични бази на територията на Пакистан и да се предадатзаподозряните в организирането на серията терористични актове в Мумбай.

През март 2010 г. беше обявено, че компютърните атаки срещу западни институции, тръгващи предимно от Китай, са се увеличили изключително много през последните месеци, което според експерти означава, че вече се води истинска кибервойна, писа в. „Таймс".

Тези и други данни са станали причина в НАТО и ЕС да се вземат извънредни мерки за защита на специалните материали, особено тези с разузнавателни данни. Според анализатори Западът няма ефикасен отговор, а ЕС е особено застрашен, тъй като киберзащитата е оставена в ръцете на страните членки.

Това е бил и единият от основните въпроси на срещата на високо равнище на страните членки на НАТО, проведена в Лисабон през октомври 2011 г.

От публикувано съобщение от 19 януари 2009 г. става ясно, че Военното министерство на Великобритания разследва голям пробив в сигурността на армията от страна на неизвестни хакери. Трафикът на електронната поща от редица бази на Кралските военновъздушни сили е бил пренасочен към руски сървър в интернет. Имейлите са били саботирани преди 13 дни, след проникването на компютърен вирус в системата на британските военни, който дори предизвика временен срив в комуникацията на мрежата.

През септември 2010 г. Иран обяви, че около 30 хил. комютри от централната компютърна система на промишлеността са атакувани с вируса „Стъкснет" (Stuxnet). Червеят е проникнал в локалната мрежа на Бушерската АЕЦ и е извел от строя центрофугите на ядрения обект в Натанзе. По данни на иранската страна , вирусът в разпространяван от компютри в Израел и от американския щат Тексас. В отговор Техеран обяви през ноември 2011 г., че също ще създаде звено за киберотбрана.

На 4 юни 2012 г. в изявление на Министерството на отбраната, Израел призна, че използва киберпространството, за да извършва нападения срещу враговете си. Признанието бе направено седмица след откриването на вируса *„Flame"* (Пламък), който по сложност и функционалност надминава всички познати до момента киберзаплахи. В текста се казва, че за първи път се разкрива документ, написан неотдавна от оперативния отдел на израелските сили за отбрана, и се посочват целите и методите на кибервойната. Израелските сили за отбрана имат непрекъсната и решителна активност с киберпространс-твото, се казва изявлението. Посочва се, че киберпространството е използвано за събиране на разузнавателни данни и ще бъде използвано за извършване на атаки и тайни операции.

Анализът на базираната в Москва „Касперски лаб" показва, че вирусът е кибероръжие, чиято сложност и функционалност надминава всички познати до момента киберзаплахи. Експертите по компютърна сигурност считат, че вируса е най-сложният зловреден софтуер, засичан до момента. Това дава основание „Флейм" да се счита за третото голямо кибероръжие, открито след вируса „Стъкснет", който атакува иранската ядрена програма през 2010 г. и вируса за кражба на данни „Дуку", кръстен на едноименния злодей от „Междузвездни войни".

През януари и септември 2012 г. цел на хакерите станаха няколко големи банки в САЩ: Bank of America, BB&T, Capital One, Citi, JPMorgan Chase. Американските власти заподозряха за това ирански хакери, свързани с правителството. Официалната власт отрича и публично осъди действията на хакерите.

В началото на юни 2012 г. компанията за компютърна сигурност „Касперски" обяви, че е открила нов вирус, използван за кражба на финансова информация. Вирусът е наречен „Гаус" и е насочен предимно към компютърните системи на Близкия изток и е сходен с вируса „Флейм".

През януари 2013 г. в. „Ню Йорк Таймс" съобщи, че в течение на четири месеца е подложен на хакерски атаки от Китай. През февруари е атакуван в. „Уолстрийт джърнъл" и сървърите на социалните мрежи Twitter и Facebook, Министрството на енергетиката на САЩ, компаниите Apple и Microsoft. За тези действия САЩ открито обвини Китай в опит да прекъсване на компютърните мрежи.

През март 2013 г. хакери за няколко дни парализираха банковата система на Южна корея. Оначало се подозираше Китай, но по-късно обвиненията се насочиха към КНДР. През май с.г. е публикуван долкад на Пентагона до Конгреса на САЩ,

в който се твърди, че Пхенян чрез кибератаки цели да получи психологическо предимство в дипломатическите отношения. По информация на южнокорейските разузнаване, в КНДР се подготвят хакери в специализирани висши военни училища. Това се отрича от Севенокорейските власти.

През периода февруари – май 2013 г. към хакерските атаки на САЩ се присъединяват и групировката на Анонимните (Anonymous), която се вмъкна в мрежите на Федералните резервна система и поличава данни до данните на 4 хил. банкови служители. Към тях се включи и „Сирийската електронна армия", която атакува западните средства за масова информация – в. „Гардиън" и „Файненшъл таймс", телевизионната компания BBC. В Twitter публикуваха фалшива новина за взрив в Белия дом, което предизвика кратковременнен срив на фондовата борса на САЩ.

В края на май 2013 г. бе публикувано, че китайски хакери са успели да проникнат в информационните бази на Австралийското разузнаване и са откраднали архитектурните планове на новостроящата се сграда на разузнаването.

Развитието на информационните технолигии неминуемо ще води до усъвършенстване на информационните оръжия и до увеличаване на техните възможности.

Потвърждение на това са думите на Скот Борг (Scott Borg – изпълнителен директор на нетърговските организации по изучаване на киберпоследствията и която се занимава с разработването на политиката на САЩ в сферата на киберзащитата) пред телевизионния канал NBC - „Киберзащитата през 2013 г. може да се определи на космическите програми през 50-те и 60-те години на XX в. САЩ, Русия и Китай водят агресивна гонитба при разработването на кибероръжия, способни да унищожат инфраструктурата. Трите страни вече са създали огромни „арсенали" от високотехнологични компютърни вируси, „троянци", червеи и други подобни, и всички тези инструменти са насочени за нанасяне на сериозни загуби чрез кокпютърно въздействие". .[33]

Особен интерес представлява *събирането на лични данни за населението на Земята*. В това направление умело се използва стремежа на хората да пазаруват - „шопингът". Натам са насочени рекламите по телевизионните и радиоканалите. А международните търговски вериги „Метро", „Кауфланд", „Карфур", „Лидал", Т-маркет", „Шел", „ОЕМВИ" с готовност ни предоставят клиентски карти за събиране на точки и да получаване на куп преференции. В повечето случаи плащането става с карта „Виза", „Мастъркард" или „Маестро". С прекарването на клиентската карта през магнитното устройство и с неизбежната усмивка на касиерката не завършва процедурата. За клиента остава скрито, че цялата транзакция се филмира от охранителни цифрови камери, плащането се регистрира, заедно с часа в който е направено, а образа на клиента се записва в базата от данни, заедно с допълнителните данни от картата. По този начин магазинът притежава лична информация за своя клиент. В тази технология няма нищо ново – тя е въведена през 50-те години на XX в. във Великобритания. Магазинът получава вашата лоялност, а вие получавате съкровените точки. Формулярът, който попълвате изисква допълнителна информация: име, адрес, възраст, възрастта на всички от семейството, e-mail, мобилен телефон и др..[34]

[33] Cheryl K. Chumley, U.S. in cyberweapons race with China, Russia, "The Washington Times": http://inosmi.ru/usa/20130221/206162855.html

[34] Джон Гиб, Кой ни наблюдава, ИК Хермес, Пловдив, 2008, с. 130-135.

След удара по Международния търговски център на 11 септември 2001 г. американските супермаркети доброволно предадоха на ФБР данни, събрани от картите за лоялни клиенти, без тяхно знание. Но това беше само началото – започна предаване на информация (лични данни) и на политици. Такива данни дават възможност на партиите да предскажат намеренията ни като гласоподаватели и им позволява да вземат решения за посланията, които да ни отправят.

Рискът от нахлуване в личното пространство нараства драматично с въвеждането на метода за автоматично идентифициране на обекти - радиочестотната идентификация *(Radio-frequency identifi-cation - RFID*) за редица продукти. Тази система използва миниатюрни компютърни чипове, с помощта на които проследяването на различни стоки от разстояние не е проблем. Известни са с името „шпионски чипове" и се поставят скрити в опаковката на стоката. Тази технология се използва от 1999 г. за предаване на информацията на разстояние от няколко сантиметра до 30 м. В момента търговците се опитват да омаловажат значението на тази японска технология, наричана още „радиобаркодове". Най-неприятното е, че шпионските чипове не могат да бъдат „убити" на касата, така че продължават да работят без огрничение във времето, без знанието на клиентите. RFID технологията противоречи на Европейското законодателство за правата на човека. Търговските интереси на фирми от САЩ и Германия се опитват да атакуват ограниченията под най-различна форма. Това е само една от разширяващата се сфера на търговия с личните данни на клиентите. С такава дейност се занимават и значителен брой частни фирми в САЩ, Обединеното кралство, Германия и страните от Югоизточна Азия.

Съществена особеност на новата среда, обаче е липсата на правителствен надзор или държавно регламентиране. Тази нова обстановка налага промени в националните стратегии за сигурност и законодателната рамка на страните, както и засилване на муждународното сътрудничество.

Заключение

Човешкият прогрес не можа да бъде спрян. Светът навлиза в мрежовия етап на своето развитие и въпросите, свързани с информационната сигурност и защитата на киберпространството ще заемат все по-значимо място в отношенията между държавите, организациите и отделните граждани. Разгледано от общоцивилизационна гледна точка, бъдещето на глобализацията на света се представя в друга светлина. Нужни са нови политики, набор от практики и възпитание, адекватно на мрежовия етап от развитието на обществото. Нужна ни **е нова парадигма** за сигурност в киберпространството в глобализиращия се свят, един изцяло нов начин на мислене и битие. В подкрепа на тази потребност Алберт Айнщайн казва: „Ние не можем да решим проблемите си с помощта на един и същи вид на мислене, което сме използвали, когато сме ги създали".

И ако искаме да направиме съвременен прочит на мисълта на древноримския историк „Ако искаш мир – готви се за война" („Si vis pasem, para bellum"), тя би гласяла по следния начин **„Ако искаш мир – готви се за кибервойна".**

НАЦИОНАЛНАТА СТРАТЕГИЯ ЗА КИБЕРСИГУРНОСТ – ИНСТРУМЕНТ ЗА ГАРАНТИРАНЕ НА СВОБОДНО И БЕЗОПАСНО КИБЕРПРОСТРАНСТВО

Васил Ст. Ризов

гр. София 1505, ул. „Черковна“, № 90, Държавна комисия по сигурността на информацията, ел. поща: dksi@government.bg; vsrizov@abv.bg

NATIONAL CYBER SECURITY STRATEGY – A TOOL TO ENSURE FREE AND SAFE CYBER SPACE

Vasil St. Rizov

ABSTRACT: *The report analyzes the current state of strategies for information and cyber security within the EU, identifies and outputs common themes and differences in the development of national cyber strategies and policies and makes recommendations on the scope and mechanisms for harmonization and provision of information interoperability in the Community.*

KEY WORDS: *cyberattack, cybercrime, cybersecurity, cybersecurity strategy, ENISA, information security*

През последните години инцидентите в областта на кибер сигурността, причинени от човешки грешки, природни явления, технически повреди или злонамерени атаки стават все по-чести, по-мащабни и по-сложни и за тях географските и политически граници са без значение.

Въпреки липсата на общо разбиране и подходи към сигурността в кибер пространството в различните страни, тя все повече да се разглежда като хоризонтален и стратегически национален проблем, който засяга всички сфери на обществото. Инструмент за подобряване на сигурността и устойчивостта на националните инфраструктури и услуги е националната стратегия за кибер сигурност (НСКС). Тя е подход към сигурността в кибер пространството на най-високо равнище, в посока отгоре надолу, при определянето на редица национални цели и приоритети, които трябва да бъдат постигнати в определен период от време, и осигурява стратегическа рамка за цялостния подход на нацията към кибернетичната сигурност.

Международната политика на Европейския съюз за кибер пространството насърчава зачитането на основните ценности на ЕС, определя стандарти за отговорно поведение, защитава прилагането на съществуващите международни закони и в кибер пространството, като подпомага държавите – членки при изграждането на капацитет за кибер сигурност и насърчава международното сътрудничество в тази област. По-долу са обобщени накратко основните регулаторни и политически документи, регламентиращи обхвата на дейностите в областта на стратегията за кибер сигурност.

В изпълнение на мисията си да подпомага разработването на синхронизирани национални стратегии за информационна сигурност, създадената през 2004 г., Европейска агенция за мрежова и информационна сигурност (European Network and Information Security Agency – ENISA) публикува мониторингов доклад за състоянието на Единното европейско информационно пространство по отношение на обхвата и акцентите на възникващата необходимост от въвеждането на единни национални изисквания за мрежова и информационна сигурност (МИС).

В доклада се прави анализ на текущото състояние на стратегии за информационна и кибер сигурност в рамките на ЕС, при който се идентифицират и извеждат общи теми и различия при разработването на национални кибер стратегии и политики и се дават препоръки, свързани с обхвата и механизмите за хармонизиране и осигуряване на информационна съвместимост в Общността.

Основният извод в доклада е необходимостта от проактивно разработване на национални програмни документи в областта на защитата и сигурността на критичната информационна инфраструктура (КИИ). Дефиниран е типичен обхват на дейности и области в една национална стратегия за сигурност на информационното пространство[3]:

- Да определи рамката и структурата за управление на сигурността в информационното пространство на национално ниво.
- Да дефинира подходящ механизъм, който да позволява на всички заинтересовани страни да участват в обсъжданията и да се споразумеят за различни мерки или ограничения, свързани с въпросите на сигурността на КИИ.
- Да изведе необходимостта от политически и регулаторни мерки, при ясно определени роли, отговорности и права на частния и публичния сектор.
- Да очертае цели и средства за разработване на национални приоритети и необходимата правна рамка, в национален мащаб и за ефективно включване в международните усилия за намаляване на последиците от престъпленията в информационното пространство.
- Да определи критерии за идентифициране и категоризиране по степени на риск на КИИ, включително ключовите активи, услуги и взаимозависимости.
- Да определи обхвата и съдържанието на оперативните документи и процедури за подобряване готовността за превенция, реакция и възстановяване, както и разработване на планове и мерки за защита на КИИ.
- Да определи систематичен и интегриран подход на националното управление на риска.

За да подпомогне държавите – членки на ЕС в разработване и поддържане на успешна НСКС, през 2012г., ENISA представи Наръчник за добри практики, който съдържа и препоръки за това как да се разработва, прилага и усъвършенства национална стратегия за сигурност в кибернетичното пространство, включва кратък анализ на текущото състояние на стратегиите за кибер сигурност в рамките на ЕС и на други места, идентифицира общи теми и различия. Процесът на създаване и управление на НСКС е разгледан в две основни фази[4]:

- разработване и изпълнение на стратегията;
- оценка и коригиране на стратегията.

Тази структура следва модела на Деминг "Plan- Do -Check -Act" (PDCA) за управление на НСКС. В допълнение, при управлението на стратегията могат да бъдат използвани следните три подхода:

- линеен подход: стратегията ще бъде разработена, внедрена и оценявана, и в крайна сметка прекратена (или заменена с друга);

- подход на жизнения цикъл: резултатите от фазата на оценка ще бъдат използвани за поддържане и коригиране на стратегията;

- смесен подход: на различните нива могат да съществуват няколко последователни цикъла за подобряване на стратегията.

Въз основа на идеи от анкети и интервюта, екипът на ENISA препоръчва подхода на жизнения цикъл, тъй като той по-добре отговаря на нуждите и характера на изискванията на НСКС.

Стратегията за кибер сигурност „Отворено, безопасно и сигурно кибер пространство“, публикувана през февруари 2013 г. като съвместно съобщение на Европейската комисия и върховния представител на Съюза по въпросите на външните работи и политиката на сигурност, представя цялостната визия на ЕС за кибернетична сигурност по отношение на пет приоритета[1]:

- постигане на устойчивост в кибер пространството;

- чувствително намаляване на кибер престъпността;

- разработване на политика за кибер отбрана и способности, свързани с общата политика за сигурност и отбрана;

- разработване на промишлени и технологични ресурси за кибер сигурност;

- създаване на съгласувана международна политика на Европейския съюз за кибер пространството и насърчаване на основните европейски ценности.

Стратегията е насочена към насърчаване на свободата и демокрацията и гарантиране на безопасното развитие на цифровата икономика в ЕС и страните – членки и в нея се посочват основните принципи, от които следва да се ръководи политиката за кибер сигурност в ЕС.

Стратегията беше публикувана едновременно с предложение за Директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза, която изисква от всички държави членки, основни доставчици на интернет и оператори на критични инфраструктури, да гарантират сигурна и надеждна цифрова среда в целия ЕС. Според предложената директива, държавите – членки трябва да приемат стратегия за кибер сигурност и да определят национален компетентен орган по кибер сигурност с достатъчно човешки и финансови ресурси, за да предотвратява, управлява и реагира в случай на рискове и инциденти в областта на МИС. Директивата си поставя следните цели[2]:

- Всички държави членки да гарантират, че са постигнали минимално ниво на национален капацитет, като са определили компетентни органи, сформирали са екипи за незабавно реагиране при компютърни инциденти (CERT) и са приели национални стратегии и национални планове за сътрудничество за МИС.

- Националните компетентни органи да си сътрудничат в рамките на мрежа, която дава възможност за сигурна и ефективна координация, включително за координиран обмен на информация, както и за откриване и отговор на равнището на ЕС. Чрез тази мрежа държавите членки следва да обменят информация и да си сътрудничат в борбата срещу заплахите и инцидентите в сферата на МИС съгласно европейски план за сътрудничество.

- Директивата цели да гарантира развитието на култура на управление на риска и на обмен на информация между частния и публичния сектор. От предприятията в

конкретните критични сектори и от публичните администрации ще се изисква да оценяват рисковете, пред които са изправени, да приемат подходящи и пропорционални мерки за гарантиране на МИС.

Прегледът на НСКС в ЕС показва, че те стават все по-интегрирани и всеобхватни, прилагат холистичен подход към кибер сигурността, като включват икономически, социални, образователни, технически, дипломатически, правни, право прилагащи, военни и разузнавателни аспекти. Държавите са изправени пред различни по трудност и характер предизвикателства. За целите на настоящото изложение съм разгледал онези от тях, от решаването на които в най-голяма степен зависи успешното разработване и прилагане на НСКС.

- Новото поколение НСКС има за цел да стимулира икономическия и социалния просперитет и да защитава кибер пространството срещу заплахи. Едно от ключовите предизвикателства при разработване на политиките за кибер сигурност днес е, осъществявайки тези цели, същевременно да бъде запазена и разширена отвореността на интернет като платформа за иновации и нови източници на растеж.

- Национална оценка за риска, която да предостави ценна информация за използването на ресурсите за разработване, изпълнение и оценка на стратегията, с конкретен фокус върху КИИ. Оценката на риска е научен и базиран на технологии процес, състоящ се от три стъпки: идентифициране на риска, анализ на риска и оценка на риска. Само след провеждане на национална оценка на риска и съгласуването на целите на стратегията с нуждите на националната сигурност, е възможно да се съсредоточи върху най-важните предизвикателства по отношение на сигурността в кибернетичното пространство.

- Ясна рамка за управление, която определя ролите, отговорностите и отчетността на всички заинтересовани страни. Стратегията за кибер сигурност ще успее само ако има ясна рамка за управление, която да осигурява форматите за диалог и координация на различните дейности, предприети през жизнения цикъл на стратегията.

- Наличието на един публичен орган или междуведомствена работна група, която да бъде определена за координатор на стратегията. Това ще бъде субект, който носи отговорността за целия жизнен цикъл на стратегията. Структурата на координиращ орган, точните отговорности и неговите взаимоотношения с другите заинтересовани страни следва да бъдат ясно дефинирани.

- Развитие на сътрудничество между публичния и частния сектор. Идентифициране и ангажиране на заинтересованите страни са ключови стъпки за успеха на стратегията. Споделянето на информация между частните и публичните заинтересовани страни е мощен механизъм да се разбере по-добре постоянно променящата се среда и форма на стратегическо партньорство.

- Установяване на основните изисквания за сигурност. Определянето на минимален набор от мерки за сигурност е сложна задача, при която трябва да се вземат предвид следните аспекти: различната степен на зрялост между заинтересованите страни, разликите в оперативния капацитет на всяка организация и различните стандарти във всеки критичен сектор.

- Създаване на способности за реагиране на инциденти. Ключово предизвикателство за правителствата е да бъдат подготвени да посрещнат евентуален сериозен инцидент в кибернетичното пространство по начин, който не подкопава откритостта на интернет. Целта на НСКС е да се повиши устойчивост и сигурността на

националните активи в областта на ИКТ, които подкрепят критичните функции на държавата или обществото като цяло.

- Противодействие на кибер престъпленията. За да бъде успешна, борбата срещу престъпленията в кибернетичното пространство изисква сътрудничество между множество участници и общности. В НСКС да се обърне основно внимание на противодействието на нарастването на престъпленията в кибер пространството, като се подготви съгласувана и координирана реакция със съответните заинтересовани страни.

Първите национални стратегии за кибер сигурност започнаха да се появяват през първите години на предишното десетилетие. Към момента 17 държави – членки на ЕС са публикували свои национални стратегии за кибер сигурност – Австрия, Белгия, Великобритания, Германия, Естония, Испания, Италия, Литва, Люксембург, Полша, Румъния, Словакия, Унгария, Финландия, Франция, Холандия и Чешката република. Първите държави в ЕС, публикували свои НСКС бяха Естония и Словакия през 2008 г., а най-нова е стратегията на Белгия от тази година. Същевременно някои страни, като Великобритания публикуваха и нови, ревизирани варианти, резултат на анализ на натрупания опит и развитието на визията за сигурността на нацията в кибер пространството.

Във всички разгледани НСКС, целта е да се повиши глобалната устойчивост и сигурността на националните активи в областта на ИКТ, които подкрепят критичните функции на държавата и на обществото като цяло. Общо е и поставянето на ясни цели и приоритети, като засилена правителствена координация на политическо и оперативно ниво, активно публично-частно сътрудничество, подобряване на международното сътрудничество и зачитане на основните ценности.

В същото време в НСКС на страните се наблюдават някои различия в подходите при реализирането на тези цели, както и при определяне на ключовите приоритети.

При Великобритания например, приоритет са националните цели, свързани с развитието на икономиката на кибер сигурността – страната да стане основната икономика за иновациите, инвестициите и качеството в областта на ИКТ в ЕС и по този начин да бъде в състояние напълно да използва възможностите и ползите от кибер пространството[5]. Също и в стратегията на Люксембург се посочва, че широкото разпространение на ИКТ е приоритет за предотвратяване на неблагоприятните въздействия върху икономиката и обществената сигурност. Отбелязва се значението на ИКТ за икономически растеж[9].

Сигурността на средата е основен приоритет за Естония, която подчертава необходимостта от сигурно кибер пространство като цяло и се фокусира върху информационните системи. Препоръчаните мерки са с граждански характер и се концентрират върху регулиране, образование и сътрудничество[7]. Словакия разглежда гарантирането на сигурността на информацията като въпрос от първостепенно значение за функционирането и развитието на обществото. Стратегическите цели на страната са насочени главно към превенцията, както и към готовността и устойчивостта на кибер средата[12].

От друга страна, Франция се фокусира върху способностите на информационни системи да се противопоставят на събития в кибер пространството, които могат да изложат на риск наличността, целостта или поверителността на данните. Поставя се ударение както върху техническите средства, свързани със сигурността на информационните системи, така и върху борбата срещу престъпленията в киберне-

тичното пространство и създаването на кибер защита[13]. Сходно е виждането в Литва, която си поставя за цел да определи целите и задачите за да се гарантира поверителността, надеждността и достъпността на електронната информация и услуги, предоставяни в кибер пространството; защитата на електронни съобщителни мрежи, информационни системи и КИИ срещу инциденти и кибер атаки; защита на личните данни и личния живот[8]. Също и в основата на стратегията на Финландия е виждането за кибер сигурността като въпрос на сигурността на данните и като задача от икономическо значение, която е тясно свързана с развитието на финландското информационно общество[11].

Формиране на съзнание за сигурност една от основните цели на НСКС на Унгария, която цели и развитие на способност за вземане на решение на политическо и професионално ниво, което може да се справи с новите предизвикателства за кибернетичната сигурност, произтичащи от технологичния напредък и гъвкаво адаптиране към тях в обозримо бъдеще[10].

Някои от страните поставят ударение върху защитата на КИИ. В своята НСКС, Германия се фокусира върху предотвратяването и разследването на кибернетични атаки, а също и върху предотвратяване на ИТ сривове и поставя основите за защита на КИИ. Използват се съществуващите разпоредби да се изясни дали и ако е така, къде са необходими допълнителни сили за осигуряване на ИТ системите, които предоставят основни функции за сигурност, сертифицирани от държавата[6]. Подобен подход наблюдаваме и в основните цели на НСКС на Чешката република – защита срещу заплахите, на които са изложени информационни и комуникационни системи и технологии, и намаляване на потенциалните последици в случай на атака срещу тях. Стратегията се фокусира върху безпрепятствен достъп до услуги, интегритет на данните и поверителността на кибер пространството на страната[14].

При прегледа на НСКС се вижда, че националните интереси са склонни да имат приоритет над общите интереси и това е подход, който трудно може да бъде променен, ако изобщо е необходима промяна. Освен това, при прегледа на различните национални стратегии за кибер сигурност се очертава и едно друго общо разбиране: докато националните политики са обвързани с границите на националния суверенитет, то стратегиите за кибер сигурност са насочени към среда, базирана на инфраструктура и функционална логика, които са независими от националните граници. Кибер сигурността е предизвикателство, което изисква международно сътрудничество, за да може успешно да бъде постигнато приемливо ниво на сигурност на глобално ниво.

В бъдещата стратегия за кибер сигурност на Република България би следвало наред с общите цели и приоритети, като зачитане на основните ценности, активно международно сътрудничество, да се отчетат и специфичните характеристики на държавата и обществото. Мерките, насочени към формиране на съзнание за сигурност и развитие на публично – частното сътрудничество например трябва да отчитат националните особености, традиции и натрупан опит в тази област. При въвеждането на регулаторни мерки следва да се отчитат интересите, както на основните участници в кибер обмена, така и на онези, които използват кибер пространството като бизнес среда.

Сигурността на онлайн средата на една нация зависи от броя на участниците с различни потребности и роли. Успешните национални стратегии за кибер сигурност трябва да вземат предвид всички заинтересовани страни, необходимостта от

осведоменост за техните отговорности и необходимостта да им бъдат предоставени необходимите средства, за да изпълняват своите задачи.

Трансграничният характер на заплахите извежда като първостепенен приоритет силното сътрудничество на общоевропейско и международно равнище, за осъществяване на ефективна подготовка не само за възпрепятстване, но и отговор на кибер атаки. Разработването и прилагането на всеобхватна национална стратегия за кибер сигурност е първата стъпка в тази посока.

Задачата за разработване на национална стратегия за кибернетична сигурност е комплексна задача. Мерките за справяне с кибер заплахите могат да бъдат политически, технологични, правни, икономически, управленски или военни по характер. Също така, всяка от предвидените мерки за сигурност трябва много последователно да бъде балансирана спрямо основните права и свободи и да бъде взето предвид нейното въздействие върху икономическата среда. Накрая, важно е да се разбере, че сигурността на кибер пространството не е изолирана цел, а по-скоро система от защитни мерки и отговорности, за да се гарантира функционирането на отворени и модерни общества.

Използвана литература

1. Върховен представител на Европейския съюз по въпросите на външните работи и политиката на сигурност, Съвместно съобщение до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите, JOIN(2013) 1 final, Брюксел, 2013
2. Европейска комисия, Предложение за директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза, COM(2013) 48 final, Брюксел, 2013
3. National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyber space, www.enisa.europa.eu, 2012, pdf
4. National Cyber Security Strategies - Practical Guide on Development and Execution, www.enisa.europa.eu, 2012, pdf
5. The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, www.gov.uk, pdf
6. Cyber Security Strategy for Germany, www.bsi.bund.de, pdf
7. Estonia, Ministry of Defence, Cyber Security Strategy, www.kaitseministeerium.ee, pdf
8. Government of The Republic of Lithuania, Programme for the development of electronic information security (cyber security) for 2011-2019, www.ird.lt, pdf
9. Luxembourg's Stratégie nationale en matière de cyber sécurité, www.mediacom.public.lu, pdf
10. Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary, www.nbf.hu, pdf
11. Finland's Cyber Security Strategy, www.defmin.fi, pdf
12. National Strategy for Information security in the Slovak Republic, www.vlada.gov.sk, pdf
13. Information systems defence and security, France's strategy, www.ssi.gouv.fr, pdf
14. Cyber Security Strategy of Czech Republic for the 2011-2015 Period,www.cybersecurity.cz, pdf

ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ В КИБЕРПРОСТРАНСТВОТО

Десислава А. Николова

Комисия за защита на личните данни

PERSONAL DATA PROTECTION IN CYBERSPACE

Desislava A. Nikolova

Commission for Personal Data Protection

ABSTRACT: *Development of new communication and information technologies and particularly the Internet and social networks pose new challenges to communication between people and the protection of personal data and privacy.*

KEY WORDS: *cloud computing, big data, data controller, data processor, data protection principles and rules, accountability, supervisory authorities*

Всеки ден милиони граждани по света използват глобалната мрежа. Банкирането от вкъщи, пазаруването онлайн и използването на социални мрежи е нормално ежедневие за много от нас. Изграждането на информационната инфраструктура обхваща основните обществени сектори като икономика, енергетика, комуникации, но и такива дейности като услугите, които са от първостепенно значение за оцеляването на човека – доставка на храна, вода, здравеопазване и транспорт.

Всеобхватното приложение на информационните технологии създава сложни взаимосвързани и взаимозависими мрежи. Потреблението на онлайн услуги нараства непрекъснато и те започват да придобиват съществено значение в съвременния свят.

В резултат – днес данните са навсякъде около нас. Масивите от данни в световен мащаб нарастват с 50% всяка година. 90% от данните са генерирани само през последните две години[1]. Големите масиви от данни (big data) предполагат развитието на съвсем нов поглед върху понятието „данни“, а именно, че данните вече са стойност сами по себе си, те са основна „стока“ на съвременната дигитална икономика.

На фона на тази положителна тенденция в технологичното развитие – социалните мрежи, облачните технологии, бързият достъп до онлайн услуги – остро се открояват и предизвикателствата, свързани със защитата на личните данни. Все почесто правото на лична неприкосновеност и принципите, на които се основава то – данните да се обработват справедливо, коректно и законосъобразно, резонира в публичното пространство във връзка със зачестили практики на неоторизиран достъп, предаване и публикуване на данни, нарушения в сигурността, както и нарушаване правото на информираност на лицата. Също така, големите масиви данни създават проблеми и предпоставки за извършване на профилиране като нов вид дейност по обработването.

[1] http://www-01.ibm.com/software/data/bigdata

Българското законодателство в областта на защитата на личните данни се стреми да въвежда принципи и правила, които да са приложими към интернет средата, отчитайки нейната основна и най-важна характеристика – запазването на интернет като свободно пространство.

Този доклад разглежда основни проблеми пред неприкосновеността с оглед събирането, генерирането и обработването на големи масиви от данни при предоставянето на облачни услуги, и предлага обобщени решения и препоръки за по-ефективно овладяване и регулиране на съществуващите процеси. Предложените механизми за реакция се базират на националната и международна практика на органите за защита на данните.

Основни понятия

Търсенето на отговори на въпросите, които поставя новото поколение технологии, трябва да започне с анализ на самите феномени, предмет на този доклад – облачните услуги и големите масиви от данни. Дефинирането им дава възможност за проследяване на процесите и механизмите, свързани с тяхното управление и използването на ресурсите. Не на последно място, разглеждането им в по-задълбочен план, спомага за идентифициране на ролите, отговорностите и сегментите, които пораждат риск, респективно се нуждаят от засилен контрол.

Облачни технологии

Според определението на Европейската агенция за мрежова и информационна сигурност ENISA (European Network and Information Security Agency), работата в облак (cloud computing) е модел на „услуга при поискване" за предоставяне на IT ресурси, основаваща се на виртуализация (virtualization) и технологии за разпределена обработка (distributed computing technologies).

На практика, предизвикателството пред европейското законодателство е, че облачните технологии предполагат доставчиците да предлагат обработване, и в частност, съхранение на данни в сървъри, които са извън територията на Европейския съюз и Европейското икономическо пространство.

Има различни роли и фактори, влияещи върху процесите в облака:

- Собственици на данни.
- Администратори и обработващи данни.
- Различни входни точки в облака.
- Доставчици на интернет услуги.
- Физическо местоположение на сървърите.

Големи масиви от данни

В областта на информационните технологии, това е понятие за описване на набор от данни с размери, надхвърлящи способността на обичайно използваните софтуерни инструменти да извличат, организират, управляват и обработват данни в рамките на допустимото време.

На практика, големите масиви от данни представляват голямо количество данни, съхранени на множество сървъри и устройства, често свързани с облачните технологии, което трудно може да се обработи с използване на ръчни или конвенционални средства за управление на бази данни.

Процесът включва обобщаване, консервация, съхранение, търсене, споделяне, анализ и визуализация. Тенденцията към обработването на все по-големи масиви от данни се дължи на необходимостта допълнителната информация да се извлича чрез анализ на един голям набор от данни, свързани помежду си. За извършването на сравнителния анализ, данните се разделят на малки групи с общ размер, което позволява да се намери корелацията за бизнес тенденциите, да се определи качеството на научните изследвания, да се използва с цел превенция на заболяванията, борба с престъпността и т.н. Големите масиви от данни предполагат възможност за използването им в разрез с основните принципи на неприкосновеността на личния живот. Те могат да се използват също и по начин, който директно да засегне лицата. Съществуват техники за изготвяне на профили и предсказване на поведението на отделни индивиди или групи чрез компилиране и анализиране на лични данни, събрани от различни източници.

На практика, събраните данни са като части от пъзел, които, подредени, дават цялостна картина, която не само индивидуализира лицето, но и разкрива информация относно неговата психика, поведение и навици.

Администратор на лични данни

Определението на понятието „администратор“ съгласно европейското законодателство и в контекста на облачните технологии, съдържа три основни компоненти:

- „физическо или юридическо лице, държавен орган, агенция или друг орган“;
- „който сам или съвместно с други“;
- „определя целите и средствата на обработка на лични данни“.

Обработващ лични данни

По силата на българския Закон за защита на личните данни, администраторът може да обработва данните сам или чрез възлагане на обработващ данните. Когато е необходимо по организационни причини, обработването може да се възложи на повече от един обработващ, включително с цел разграничаване на конкретните им задължения. Новото предложение за европейски Регламент за защита на личните данни доразвива понятието, като се дискутира включването на следните уточняващи характеристики: обработващият лични данни трябва да предостави достатъчни гаранции, че ще приложи подходящи технически и организационни мерки и процедури, така че обработването да отговаря на законодателните изисквания и да гарантира защитата на правата на субекта на данни. Той действа единствено по указания на администратор и включва друг обработващ лични данни единствено с предварителното разрешение на администратора.

Трето лице

"Трето лице" е физическо или юридическо лице, орган на държавна власт или на местно самоуправление, различен от физическото лице, за което се отнасят данните, от администратора на лични данни, от обработващия лични данни и от лицата, които под прякото ръководство на администратора или обработващия имат право да обработват лични данни.

За целите на доклада, като основни понятия ще маркираме също принципите: *неприкосновеност (privacy)*, *отчетност (accountability)*, *правото да бъдеш забравен (right to be forgotten)*, *видимост и прозрачност (visibility and transparency),* наличност *(availability).*

Проблеми и предизвикателства

Общите проблеми са свързани с изискването за еднакво разбиране на неприкосновеността, заплахите, мерките и средствата за защита и липсата на единни стандарти за защита. Новото поколение технологии поставят за отговор множество въпроси и основни предизвикателства:

- Запознати ли са потребителите със заплахите в мрежите?
- Как се използват личните данни от потребителите, от доставчиците на услуги и какви са параметрите за настройка?
- Кой от правна гледна точка е администратор и кой обработващ лични данни, както и кой каква отговорност носи?
- Как трябва да се организира отчетността на действията?
- Каква е границата между публичност и неприкосновеност?
- Каква е ролята на надзорните органи и какви са възможностите за съвместни действия и прилагане на общ подход на международно ниво?

В голяма степен, предизвикателство пред големите масиви от данни е и използване на данни за други цели. Тази практика противоречи на два от основните принципи за защита на данните, че събраните данни не могат да бъдат използвани за цели, които са несъвместими с целите, за които са събрани първоначално (принцип за ограничаване на целта) и както и на принципа на пропорционалност. В този ред на мисли, използване на данни за други цели, крие рискове относно качеството и точността на данните – също част от основните принципи за защита.

Друг проблем, свързан с големите данни е тенденцията към максимизиране на събираните данни, доколкото те се разглеждат като стойност, която може да е свързана с бъдещи ползи.

Липсата на прозрачност относно това как данните се събират и обобщават води до нарушаване на друг основен принцип – правото на достъп и контрол от страна на потребителите върху обработването на лични данни.

Не на последно място, компилирането и обобщаването на данни от различни източници разкрива чувствителна информация за дадено лице и може да доведе до цялостно профилиране на вече идентифицирано лице.

От свое страна, интернет търсачките също предоставят възможност за събиране на големи масиви от данни и профилиране. Крайните потребители имат малко възможности за оказване на влияние върху големите мултинационални компании, предлагащи услугата „търсене“. Като пример може да се посочи решението на Съда на Европейския съюз по дело, свързано с „правото да бъдеш забравен“. Делото е относно жалба на испански гражданин пред Агенцията за защита на данните срещу голям испански всекидневник, срещу Google Испания и Google Inc. Жалбата е по повод на това, че след като се въведе името му в интернет търсачката на Google, списъкът от резултатите показват връзка към две от страниците на въпросния ежедневник, където е публикувана обява за принудително събиране на вземания, предприето срещу него за задължения в областта на социалното осигуряване.

Съдът на ЕС отсъжда в полза на лицето и задължава Google да заличи от списъка на резултатите връзки с уебстраници, публикувани от трети лица и съдържащи информация за въпросното лице.

„Правото да бъдеш забравен“ като концепция е предвидено в настоящата законодателна реформа, като ще обхваща цялостното предоставяне на интернет услуги, включително по отношение на социалните мрежи.

От гледна точка на надзорната дейност на органите за защита на данните спрямо основните действащи фигури в процеса на предоставяне на облачни услуги, се наблюдават две основни предизвикателства.

1) Първото предизвикателство обхваща обработването и защитата на данни на собствена територия. Някои организации, например доставчици на интернет услуги, правителството и други, обработват голямо количество данни като използват техните собствени центрове за данни с множество сървъри, устройства за съхраняване и устройства за поддържане на резервно копие на информацията.

Извършването на проверки за целите на защитата на лични данни се разглежда в два аспекта:

От правна гледна точка проверяващи (одитори в сферата на неприкосновеността, представители на надзорните органи) контролират изпълнението на правните изисквания като например договори относно обработването на данните, вътрешни правила, списъци за достъп до данните, процедури за техническа и организационна защита на данните. Проверяващите органи също така могат да разпитват служители, да проверят лог-файловете, а също така да извършват (ограничен) анализ на съхранените данни.

В технологичен план проверяващи със специализирано познание по хардуер и софтуер (операционни системи, софтуер за back-up поддръжка, приложения за бази данни и др.) провеждат щателни разследвания на (големи масиви) данни, които се използват във всеки конкретен случай.

2) Второто предизвикателство обхваща обработването и защитата на данни на територия извън Европейския съюз, тоест процесът на предоставяне на данни към администратори и/или обработващи в друга страна. Този процес може да бъде онагледен със следната схема:

> Клиент (физическо лице) → Лични данни → Администратор в друга държава (този модел включва ситуация, в която даден потребител използва *Facebook*).

> Клиент (физическо лице) → Лични данни → Национален администратор → Лични данни → Обработващ в друга страна.

Прекият контрол от страна на националния надзорен орган или други органи по отношение на обработването на данни в чуждестранната компания е възможен ако е предмет на регламентация в съответния договор за обработване в облака. В подобни случаи контролът е възможен единствено чрез неофициални средства за сътрудничество с чуждестранния надзорен орган (ако има такъв). Наличието на договор за двустранно сътрудничество между органите за защита на личните данни също спомага за предприемането на съвместни действия.

Действащата европейска правна рамка в областта на неприкосновеността поставя редица изисквания пред администратори на лични данни, които предоставят услуги в други държави:

- предоставяне на данни на трети страни (които не са членки на ЕС) е позволено единствено ако надзорният орган за защита на данните констатира, че е налице адекватност на защитата на личните данни в дадена трета страна;
- страната в която ще се предават данните има адекватно ниво на защита, определено с решение на Европейската комисия.

В рамките на Европейския съюз действат принципите на единния вътрешен пазар и се гарантира свободното движение на данните.

От практическа гледна точка обаче, възникват редица въпроси и предизвикателства във връзка с предоставянето на данни в трети страни. Органите за защита на данните не могат да проверяват, дали личните данни са надеждно защитени на техническо ниво, особено ако данните са обработвани от обработващ на чужда територия, извън тяхна юрисдикция. Затова от съществено значение е наличието на договор между местния администратор на лични данни и обработващите в трети страни.

Обработването в контекста на предоставянето на данни в трети страни, се сблъсква също и с предизвикателствата на различните национални юрисдикции, респективно различното правно третиране на взаимоотношенията между отделните участници в процеса.

В списъка с предизвикателства пред правната защита на личните данни, в контекста на облачните технологии, трябва да се включи и адекватната реакция при нарушения в сигурността на данните. Важна крачка напред в преодоляването на тези предизвикателства е приемането на Регламент 611/2013 относно уведомяването при нарушения в сигурността на данни, по който Комисията за защита на личните данни е компетентен орган.

Препоръки и възможни решения

С оглед на изложените по-горе проблеми и предизвикателства, решения могат да се търсят в следните посоки:

1. Необходимост от еднакво разбиране по отношение на това кой е администратор и кой обработващ данни при предоставяне на облачни услуги с оглед уточняване на техните права и задължения.
2. Повишаване на отчетността на обработващите данни спрямо администраторите и задълженията за въвеждане от тяхна страна на технически и организационни мерки за защита. Това може да коригира наблюдавания дисбаланс при обработването в облак, при който клиентът (особено ако е малко или средно предприятие) може да изпита затруднения при упражняването на пълен контрол съгласно законодателството в областта на защитата на данни по отношение на начина, по който доставчикът извършва поисканите услуги.
3. Разпределението на отговорностите между администратор и обработващ да се уреди в договор, който да съдържа клаузи за защита на личните данни, и в който ясно да са разписани:

- задълженията на страните;
- правата на лицата (в т.ч. правна защита), както и гарантиране правото на достъп на физическите лица до техни данни, включително каква информация се обработва за тях и за какви цели;

- възможност за упражняване на контрол от страна на компетентния надзорен орган върху компанията, която предлага облачни услуги (администратор или обработващ);
- процедура, гарантираща „правото да бъдеш забравен“;
- срокове за задържане на данните;
- обвързването на подизпълнителите с клаузите по основния договор между администратор и обработващ;
- ясни правила по отношение съхраняването и процеса по заличаване на данните (не само изтриване на данните, но и заличаване от сървъра);
- процедура за уведомяване при нарушаване сигурността на данните, както и за уведомяване на компетентния надзорен орган и засегнатите лица;
- описание на наличието на сървъри за поддържане на резервни копия на данните и тяхното местоположение, като към тези устройства следва да се прилагат идентични технически и организационни мерки за защита.

4. По отношение на изпълнителните правомощия, надзорният орган следва да може да проверява, както документацията и политиката по неприкосновеността, така и лог-файловете.

5. Необходимо е да се обърне специално внимание на проблемите, свързани с обработването на бази данни и услуги, съдържащи така наречените „чувствителни данни“. Следва да се предвидят специални предпазни мерки, така че съобщаването, обработването и съхранението на данни извън националната територия да не изложи на неприемливи рискове сигурността и неприкосновеността на личния живот на гражданите, националната сигурност и икономика. Съгласно Закона за защита на личните данни по принцип е забранено обработването на лични данни, които разкриват расов или етнически произход, както и политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, или се отнасят до здравето, сексуалния живот или до човешкия геном.

6. Да се работи в посока въвеждане на единни стандарти в областта на неприкосновеността на международно ниво и уеднаквяване на нивото на защита на личните данни между отделните страни. Това може да стане чрез разработването на международен правен инструмент, като например отделен протокол към член 17 на Международния пакт за гражданските и политическите права на ООН.

7. Да се търсят възможности за по-задълбочено сътрудничество между отделните органи за защита на данните на оперативно ниво.

8. Компаниите да разработят ясна и разбираема политика по неприкосновеността и да се извършва оценка на риска.

9. Да се изисква категорично и информирано съгласие от субектите на данни във връзка с използването на техни лични данни, вкл. за целите на профилирането.

10. Да се използват подходящи техники за анонимизиране и псевдонимизиране на данните.

11. Да се гарантира по-голяма прозрачност и контрол върху процедурите по събиране и обработване на лични данни. Лицата трябва да получават информация относно вида на събираните данни, тяхното обработване, целите за които се събират и дали данните ще се предоставят на трети страни.

12. По-добро справяне с предизвикателствата пред неприкосновеността чрез прилагане на механизма „неприкосновеност при проектиране“.

13. Прилагане на принципа на самоочетност на администраторите (accountability).

14. Повишаване на осведомеността на обществото.

Насоките за подобряване и развитието на защитата на данните трябва да обхващат обучение на всички нива, дискусии, засилване на взаимодействието между специалистите (най-вече между юристи и информатици) и осъществяване на добро взаимодействие между всички заинтересовани страни на национално и наднационално равнище.

Като добра национална практика за сътрудничество за защита на личните данни в областта на киберсигурността, може да се посочи сключените споразумения за сътрудничество в областта на информационните технологии между Комисията за защита на личните данни с Министерството на вътрешните работи и Държавната агенция „Национална сигурност“. При всички констатации за киберпрестъпления, българският надзорен орган за защита на данните изпраща въпросът на компетентните правоприлагащи органи.

Заключение

Новите интернет възможности са преимущество и улеснение в различни сфери от живота, но също така създават и редица опасности пред личната неприкосновеност. За намиране на адекватни отговори и правилни решения е необходима превенция, активна позиция и повишаване на взаимодействието между:

- Държавните структури;
- Университетите и научните организации;
- Структурите на бизнеса;
- Неправителствените организации и медиите.
- Гражданите.

Литература:

[1] Директива 95/46/ЕО на Европейския Парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни.

[2] Закон за защита на личните данни.

[3] Закон за електронните съобщения.

[4] Регламент 611/2013 на Европейската комисия относно мерките, приложими за съобщаването на нарушения на сигурността на личните данни съгласно Директива 2002/58/ЕО.

[5] Предложение за регламент на Европейския Парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (общ регламент относно защитата на данните).

[6] Working Paper on Big Data and Privacy. Privacy principles under pressure in the age of Big Data analytics, 55th Meeting, 5-6 May 2014, Skopje.

[7] Становища на Работната група по чл. 29:

Opinion 03/2013 on purpose limitation - WP 203 (02.04.2013)

Opinion 05/2012 on Cloud Computing - WP 196 (01.07.2012)

[8] Милина В., 2013 г., Киберсигурността – стратегически национален проблем, IT4Sec Reports 108 (София, Институт по информационни и комуникационни технологии), http://dx.doi.org/10.11610/it4sec.0108

[9] Решение по дело C-131/12 Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González, www.curia.europa.eu

[10] Matjaz Drev, Katarina Medved, Reflection on some of the challenges regarding protection of big data

[11] Prof. Veselin Tselkov, Mariya Mateva, 2014, Central Eastern Europe Data Protection Authorities, 16th Meeting, Skopje, Cloud Computing, Big Data, Accountability and new challenges for Protection of Personal Data.

КИБЕР АТАКИ И СЪВРЕМЕННИ ПОДХОДИ ЗА ЗАЩИТА

Димитрина Л. Полимирова

Национална лаборатория по компютърна вирусология – БАН,
София 1113, ул. „Акад. Георги Бончев“, блок 8, офис 104
dimitrina.polimirova@nlcv.bas.bg

CYBER ATTACKS AND MODERN APPROCHES FOR PROTECTION

Dimitrina L. Polimirova

***ABSTRACT**: In this report main problems related to the attacking processes in cyberspace are discussed. Special attention of the changes in the attacking tools is paid. At the end, the potential damages from cyber-attacks accomplished to computers, systems and networks as well as current approaches and means of prevention and protection from cyber-attacks are also discussed.*

***KEY WORDS**: Cyber Security, Information Security, Data Security, Malware*

Киберпространството е възникнало като понятие през последните петнадесетина години и представлява обобщен израз на изградената от съвременното общество информационна инфраструктура, включваща всички йерархични нива на съвременната глобална мрежа.

Причините за това съотношение са много и най-различни, но доминиращото е особената невидимост на информационните престъпления, състояща се в това, че престъпление има, но извършител няма, тъй като доказателства за пряката отговорност се намират изключително трудно.

Терминът кибер война (Cyber-warfare) се използва в сферата на компютрите и Интернет и представлява съвкупност от дейности, свързани с войната в кибер пространството [2].

Още от времето на Студената война остана практиката да се организират тайни дейности от разузнавателните агенции, свързани с периодично тестване на Интернет/Интранет мрежите за слаби места. В тази връзка е необходимо да се отбележи,

че техниките за проучване на слабите места в Интернет и глобалните мрежи нарастват лавинообразно с всяка измината година.

Кибер контраразузнаването е свързано с определяне на мерки за идентифициране, за проникване и за неутрализиране на външни действия [3]. Кибер инструментите са приложими под формата на стандартни търговски практики, в резултат на което чуждите разузнавателни агенции могат да получат сериозни информационни резултати. Новите кибер инструменти допълват великолепно традиционните класически методи за събиране на информация.

Комуникацията и информацията сигурност станаха ключов фактор в развитието на икономиката и обществото. Понастоящем мрежите и информационните системи са се превърнали в необходими спомагателни услуги, които "доставят" данни в степен, немислима допреди години. Тяхната готовност за работа е критична за останалите инфраструктури като например водоснабдяване и електроснабдяване. Тъй като всички, и бизнесът, и частните лица, и публичната администрация искат да използват възможностите на комуникационните мрежи, то сигурността на тези системи се превръща в необходимо предварително условие за по-нататъшен прогрес.

1. АТАКУВАЩИ ПРОЦЕСИ В КИБЕРПРОСТРАНСТВОТО

1.1. Промени в атакуващите инструменти за последните години

Malware (образувана от “malicious” – злонамерен и “software” – софтуер) е софтуер, проектиран да проникне или повреди компютърната система без официалното съгласие на собственика й [1]. Изразът се използва главно от компютърни специалисти и има смисъл на различни форми на враждебен, натрапчив или досаден софтуер или първичен (програмен) код.

Много компютърни специалисти не са запознати с термина и много често употребяват израза “компютърен вирус” за всички типове злонамерен софтуер, включително и за самите вируси.

Злонамереният софтуер включва компютърни вируси, червеи, троянски коне, повечето rootkit-ове, шпионски софтуер (spyware), измамнически рекламен софтуер (adware), измамнически криминален софтуер (crimeware) и т.н.

През 80-те и 90-те години стана ясно, че злонамерените програми са били създадени като форма на вандализъм или шега. По-късно по-голямата част от злонамерения софтуер е бил написан с намерение за финансова изгода. Това може да се възприеме като начин авторите на злонамерен софтуер да материализират контрола, който притежават над заразените системи (и така да превърнат този контрол като източник на финансови приходи).

Към настоящия момент една от най-често използваната форма на злонамерен софтуер, прилагана за печелене на пари, е известна под името шпионски софтуер (spyware). Шпионският софтуер е комерсиален продукт, чийто цели са събиране на информация за потребителите. Това става като се показват изскачащи прозорци с реклами или като се променя поведението на уеб-браузъра с цел финансова изгода. Например някои шпионски софтуер пренасочват резултатите от търсачките към платени реклами.

Шпионският софтуер се инсталира понякога като един или друг вид Троянски кон. Spyware-ът се различава с това, че създателите му се представят открито като хора от бизнеса (например като продавачи на рекламно място в изскачащи прозор-

ци (pop-ups), създадени от автора на злонамерения софтуер). Повечето от тези програми имат лицензионно споразумение, което предпазва създателя от преследващи законови действия.

Други, наричани от медиите крадящ софтуер "stealware", променят кода на афилиейтния маркетинг и така доходите от реклама отиват в създателя на злонамерения софтуер, а не до истинския получател.

Възможност на авторите на шпионски софтуер да създават финансова облага чрез техния софтуер е и възможността директно да използват заразения компютър, за да свършат някаква работа. Спам вирусите като тези от фамилията на Sobig и Mydoom са използвани от спам индустрията. Заразените компютри се използват като проксита, за да изпращат спам съобщения. Предимството да се използват заразени компютри е в това, че те са ужасно много (благодарение на злонамерения софтуер) и те осигуряват анонимност на спамерите, което пък ги защитава от преследване от закона.

За да координират действията на много заразени компютри, атакуващите използват координиращи системи, известни като botnet-и. При тях е възможно атакуващият да даде инструкции до всички заразени системи едновременно с определена цел. Botnet-ите могат да бъдат използвани и за актуализиране на злонамерения софтуер на заразените системи. По този начин ги правят устойчиви на антивирусния софтуер и софтуера, свързан със сигурността.

И на края, чрез шпионския софтуер може да се откраднe директно от потребителите, чиито компютри са заразени. Някои злонамерени програми инсталират т.н. keylogger, който копира и записва всички действия на потребителя по време на вписването на паролата, информация за кредитни карти или друга лична информация, която може да бъде от полза на авторите на шпионски софтуер. Тази информация се изпраща автоматично на автора на шпионския софтуер, което му дава възможност например да краде от кредитни карти.

1.2. Атакуващи процеси в глобалната мрежа

Кибер шпионажът е действие или процес на събиране на секретна информация от отделни индивиди, конкуренти, групи, правителствени организации и военни и политически противници, използващи незаконно инструменти през интернет, мрежи, софтуер или компютри.

Уеб вандализъм може да бъде описан като атаки, които променят съдържанието на уеб-страници. Атаките от този тип са осъществени без задълбочена подготовка и обикновено не причиняват големи вреди.

Друг често срещан процес в глобалната е мрежа е **събирането на данни**, при който поверителна информация, която не се пази добре, може да бъде засечена и дори по-лошо – модифицирана, и по този начин да бъде полезна за шпионите на противника.

Една от най-разпространените атаки към корпоративни сървъри са **атаки от тип разпределен отказ от услуга** (Distributed Denial of Service (DDoS)). При тях голям брой компютри в една страна осъществяват разпределена атака от тип отказ от услуга (Denial of Service (DoS)) срещу други компютърни системи в други страни.

Критичните инфраструктури също са уязвими от страна на кибер атаки.

Не бива да се пренебрегва възможността за **подправяне (компрометиране) на хардуера**, използван в компютрите и мрежите. Възможно е да бъде скрито злонамерено съдържание в оригиналния софтуер, вътрешното програмно осигуряване (firmware) или дори в множеството на инструкциите на микропроцесорите.

2. ПОТЕНЦИАЛНИ ВРЕДИ ОТ КИБЕРАТАКИ

2.1. Неоторизиран достъп до компютри и компютърни мрежи

При провеждане на кибер атаки в зависимост от сценария, който се реализира, се набелязват различни цели, като една от най-важните е постигане на частичен или пълен достъп до определени ресурси в локално или отдалечено позиционирани компютри и компютърни мрежи.

Неупълномощените и незаконни действия от страна на атакуващия хакер са в състояние да причинят изключителни материални и нематериални щети.

2.2. Злонамерено изпълнение на програми за модифициране или разрушаване на данни, кибервандализъм

Следващият основен момент в сценариите за информационните атаки в киберпространството (Information Cyber Attacks) е идеята за безсмисленото и сляпо разрушение, за извършване на сериозно планирани и много внимателно проведени поредица от действия, често наричани с общото описателно название кибервандализъм.

В стотиците публично известни сценарии на кибер атаки много малък процент заемат разрушителните варианти, като при това трябва да се направи уговорката, че в повечето от случаите това се явява защитна мярка от страна на хакерите, които прибягват до разрушение с цел да прикрият своите следи.

Злонамереното изпълнение на програмни единици в атакуваната операционна среда, което цели модифициране на данни, е със значително присъствие в сценариите за информационните атаки в кибер пространството (Information Cyber Attacks), тъй като едно незначително въздействие в избраната посока върху определен информационен масив може да доведе до важни последствия.

Това определя високата мотивираност на определени финансови групировки да създават и поддържат подобни хакерски екипи, чрез които има възможност да се влияе по незаконен начин на бизнеса с определени суровини и стоки.

Възможностите за преодоляване на тази много сериозна и актуална заплаха за световната дигитална икономика са добри, но изискват изграждане на система от превантивни действия още в момента, когато започва да се планира създаването на следващата УЕБ-базирана информационна система, която служи за създаване и управление на реални парични потоци.

2.3. Лъжлива или злонамерена информация за идентичността на потребители

Сравнително често се случва в т.нар. електронно досие на отделен гражданин или служител във фирма да се осъществи подмяна на данни в отделни полета, или да бъде подменено тотално цялото досие.

Специално внимание тук трябва да се обърне на обстоятелството, че докато не се възстанови състоянието на базата, например, чрез резервни копия, ако има такива, или чрез сканиране на съответни оригинали, пострадалите потребители са на-

пълно лишени от всякакви ресурси, което в случай на данни, свързани със здравословното им състояние, може да се окаже много опасно.

Известни са също така и успешни опити на хакерски атаки, имащи за цел манипулиране на отделни информационни полета, на отделни информационни единици и на цели информационни потоци към, от и на сателитните системи.

3. СЪВРЕМЕННИ ПОДХОДИ И СРЕДСТВА ЗА ПРЕВЕНЦИЯ И ЗАЩИТА ОТ КИБЕР АТАКИ

3.1. Методи и средства за защита на мрежи и канали за връзка

В общата стратегия за защита от хакерски атаки основна роля играе защитата на информационната инфраструктура, съставена от т.нар. технически средства, в която влизат компютрите, мрежите и каналите за връзка.

При изграждането на защитна схема срещу хакерски атаки се включват следните етапи: 1) подготовка на трасето; 2) подготовка на средата; 3) подготовка на сигналите; 4) подготовка на модулите; 5) подготовка на компютрите.

3.2. Методи и средства за защита на софтуерни системи

Поради високата сложност на тези компоненти и поради тяхната вътрешна структура, която е съставена от стотици и понякога хиляди модули, то практически е невъзможно да се изгради и изпълни една наистина защитена от кибер атаки софтуерна система.

Независимо от това, за да се гарантира приемливо ниво на защита, е необходимо да се извършат следните подготовки: 1) подготовка на операционната система; 2) подготовка на драйверите; 3) подготовка на приложенията.

3.3. Повишаване на сигурността при достъп до интернет приложения

Основната причина за проблемите по сигурността в съвременните компютърни системи е съществуването на Интернет, тъй като от основна входно-изходна точка за добронамерените информационни потоци, Интернет се превръща и в основна входно-изходна точка за злонамереното мислене.

Една от сравнително лесните за реализиране и с висок защитен потенциал операция срещу хакерските атаки е внимателното преглеждане на опциите на всички Интернет приложения и настройването им в посока на един консервативен профил.

Следваща в операциите за повишаване на сигурността трябва да бъде включването и активното използване на отделните средства за криптиране на съдържанието и на отделните протоколи в мрежовите сесии.

По-нататък трябва да се продължи с активното използване на всички налични средства за електронен или цифров подпис, като специално внимание се отдели на използването на максимална дължина на всички ключови стрингове и пароли.

Особено внимание трябва да се отдели на местата и поводите за обявяване на електронните адреси, тъй като чрез електронната поща се реализира една значителна част от подготовката на сценариите за атакуващи действия.

Допълнителни грижи трябва да се отделят на информацията, която се появява през различните етапи на браузване в т.нар. статусни линии на текущо използвания браузър, тъй като значителна част от хакерските атаки са реализирани под формата на манипулирани хипервръзки или манипулирани WEB адреси.

3.4. Повишаване на сигурността на данните

Когато се търси тотално гарантиране на сигурността и защита срещу кибер атаки, не бива в никакъв случай да се забравя значението на данните.

Това е така, защото данните са най-променливия информационен поток във функционирането на една информационна инфраструктура и поради това са най-силно изложени на възможността за реализиране на хакерска атака чрез тях.

Основният принцип за опазване на данните, който трябва да се спазва, е тяхното непрекъснато и постоянно опаковане или архивиране. Освен това е необходимо при тези процеси непрекъснато да се използват сигурни крипто алгоритми с голяма дължина на ключовете.

Следваща стъпка е при операции в паметта с данни да се изгражда система за предварително планиране при която се гарантира присъствието на минимално количество данни за минимално време. Освен това е силно желателно данните до последния момент преди тяхното използване да се съхраняват в опакован и кодиран вид.

ЗАКЛЮЧЕНИЕ

Въпросът за сигурността е едно от големите предизвикателства, свързано с разширяващите се услуги, предлагани към граждани, корпоративни организации и държавни структури. За разлика от типичните уеб сайтове, предлагащи възможност за браузване и сваляне на големи масиви от данни, за порталите, съдържащи чувствителна персонална информация заплахата от възможно проникване или кражба на самоличност е висока и може да доведе до сериозни последици.

В тази връзка сигурността се е превърнала в стока, продавана и купувана на пазара, и е част от договорните съглашения между страните по договорите. Обикновено се прави имплицитното предположение, че ценовият механизъм ще балансира разходите за обезпечаване на сигурност и специфичната необходимост от сигурност. Въпреки това много рискове за сигурността остават без решение или решенията достигат бавно до пазара поради неговите несъвършенства. Специфични политически мерки, отнасящи се до тези несъвършенства, ще подобрят пазарните процеси и същевременно ще усъвършенстват функционирането на законовите рамки.

ЛИТЕРАТУРА

[1] Honig, A., *Practical Malware Analysis*, No Starch Press, 2012, ISBN 1593274300, pp. 2-3

[2] Shakarian, P., Shakarian, J., Ruef, A., *Introduction to Cyber-Warfare: A Multidisciplinary Approach*, Newnes, 2013, ISBN 0124079261, pp. 1-8

[3] http://www.dtic.mil/doctrine/dod_dictionary/, (последно посетен на 02 юни 2014)

ЕНЕРГИЙНА КРИТИЧНА ИНФРАСТРУКТУРА – МЕТОДОЛОГИЯ ЗА ОПРЕДЕЛЯНЕ РИСКА НА ОБЕКТИТЕ

Димчо Кънев

I. ВЪВЕДЕНИЕ

Енергията е основен елемент на съвременния начин на живот и движеща сила на икономиката. Човешкото развитие води до непрекъснатото нарастване на потреблението ѝ. Безопасната, сигурна, устойчива и икономически достъпна енергия като постоянен процес по предоставяне на жизнено необходими обществени услуги за функциониране на обществото ни заема съществено място в осигуряването на международната и на националната сигурност. Енергийните инфраструктури, захранващи с енергия сградите, които хората използват, промишления сектор и сектора на услугите, са едни от особено значимите за нормалното функциониране на обществото критични инфраструктури. През последните години рисковете и предизвикателствата пред сигурността на функционирането на тези инфраструктури нарастват значително, като чувствително е нарастването на кражбите, вандализма и кибер атаките.

В момента защитата на критичните инфраструктури е съществен елемент от политиката за сигурност на много страни, най-вече на страните, членки на НАТО и Европейския съюз. Основа за това е Европейската програма за защита на критичните инфраструктури и Директива 2008/114/ЕО на Съвета от 8 декември 2008 г. относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита.

Защитата на критичните инфраструктури е сравнително нова съвкупност от дейности за държавната администрация в страната ни, работеща по защитата на националната сигурност и защитата при бедствия. С промените в Закона за защита при бедствия (изм. и доп., бр. 80 от 14.10.2011 г.) в българското законодателство се въведоха нормативно изискванията на Директива 2008/114/ЕО. През 2012 – 2013 г. се приеха основните подзаконови нормативни актове: Наредбата за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях, с която се въвежда процедура за оценяване на критични инфраструктури и обектите им с въздействие от национален характер; Наредбата за реда за установяването и означаването на европейски критични инфраструктури в Република България и мерките за тяхната защита, с която се въвежда процедура за оценяване на европейски критични инфраструктури с въздействие от транснационален характер. Съгласно техните разпоредби при значително въздействие за страната ни от нарушаването и/или унищожаването на дадена инфраструктура тя се превръща в критична инфраструктура. Ако въздействието освен национален има и значителен транснационален характер в поне една държава-членка на Европейския съюз, критичната инфраструктура се превръща в европейска критична инфраструктура.

II. УПРАВЛЕНИЕ НА РИСКА ЗА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ

Всички критични инфраструктури имат нещо общо, а то е, че евентуални пропуски в тяхната сигурност и защита могат да застрашат здравето на населението,

околната среда, общественото доверие и дори националната и международната сигурност. Сложната взаимозависимост между инфраструктурите в различните сектори означава, че от дадено събитие може да произтече ефектът на доминото и върху сектори, които на пръв поглед не са непосредствено и явно свързани със събитието. Критичните инфраструктури се осмислят по по-различен начин като посегателството срещу тях може да не доведе до разрушения и жертви сред населението и околната среда, а да нанесе огромни щети на политиката, икономиката и др. Т.е. критичността на инфраструктурите ги превръща в стратегически ресурс, за който управлението на рисковете е приоритет.

В българското и в европейското законодателство не е определено напълно какъв е обхвата на дадена критична инфраструктура. Посочено е: "елемент, система или части от нея". Предоставен е избор за определяне обхвата на потенциалните критични инфраструктури и обектите им, който да се анализира за установяване критичността им. Национален подход е съсредоточаването върху обектите, като организационно и/или икономически обособена част от дадена критичната инфраструктура, която е ключова за нормалното функциониране, непрекъснатостта и целостта й. Ако един обект на инфраструктурата е критичен, то и цялата инфраструктура се установява за критична.

Управлението на риска е възприет в световен мащаб основен подход към критичните инфраструктури. Той обхваща всички дейности, целящи идентифициране и намаляване на рисковете, произтичащи от зависимостта на обществото от критичните инфраструктури и обектите им в случаи на бедствия, аварии, катастрофи, терористични актове. Управлението на риска е съвкупност от процеси, методи и инструменти, които осигуряват дисциплинирана околна среда и подпомагат вземането на решения за това да се определя кои рискове са първостепенни за справяне, да се преценява постоянно какво може да се обърка и да се вземат съответните мерки. Управлението на риска само по себе си не гарантира успех - то дава възможност да се вземат правилните решения, да се предвидят и предотвратят изненади, да се подобри шанса за успех. Добре информирани решения могат да се вземат само ако се разбират рисковете. Обобщената оценка на риска се основава на съчетанието на три параметъра – опасност, уязвимост и вероятност. Опасността става риск само когато е налице уязвимо място в инфраструктурата, което тя може да атакува.

Управлението на риска за обектите на сложните системи, каквито са енергийните е ключов за цялостната им защита. Съсредоточеността е върху цялата енергийна верига, от производството на енергия, през преноса и разпределението, до крайното потребление. Голямата площ, на която се разпростират енергийните мрежи и големият брой други енергийни обекти, разположени на територията на цялата страна, води като цяло до непрогнозируемост и неопределеност на средата за сигурност, в която оперира енергийната система. Това води до нарастване на уязвимите места в нея, които се характеризират с по-голяма податливост на въздействията на опасностите, а оттам и на уязвимостта на система като цялост. Такива уязвими места обикновено са лесно достъпни за опасностите, но трудни за защитаване. Поради това вероятността да се появи повреда със сериозни последствия в енергийната система е сравнително голяма. Ефективната политика на управление на риска в сектор Енергетика изисква да се постави акцент върху способността да се предвидят опасностите за енергийните критични инфраструктури, да се систе-

матизират уязвимостите им и да се минимизират рисковете, като се отчете и сложната им взаимообвързаност с останалите сектори на страната.

Методологията за определяне на риска е етап от цялостния подход, включващ установяването на критичните инфраструктури и обектите им, анализа и управлението на риска за тях и прилагането на конкретни мерки за намаляване на уязвимостта им.

III. МЕРКИ ЗА НАМАЛЯВАНЕ НА УЯЗВИМОСТТА НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ

Мерките за намаляване на уязвимостта гарантират защитата на критичните инфраструктури и обектите им от опасности, които са резултат от човешка дейност, технологични заплахи и природни бедствия, като се отдава приоритет на мерките срещу терористичните заплахи. Те прилагат подходящ контрол и средства за предотвратяване на инцидентите или намаляване на последиците от тях в инфраструктурите, като въвеждат мерки за укрепване им (физически, организационни и други).

Намаляването на уязвимостта на критичните инфраструктури и обектите им се разглежда като динамично състояние на дадена система, което осигурява непрекъснатото неутрализиране и противодействие на външни и вътрешни фактори. Главната цел е да се осигури надеждна и оптимална защита от всички възможни за критичните инфраструктури и обектите им опасности, чрез цялостно изграждане на най-подходящата структурна организация за сигурност. Тази организация трябва да изпълнява ефективно целите и задачите на сигурността, да реагира своевременно и изпреварващо при екстремни ситуации, да е оптимална и функционално самоусъвършенстваща се, да е снабдена с модерни технически средства и изградена от професионалисти. Структурната организация трябва да е разработена и съгласно действащото в страната нормативно законодателство в тази област с разбирането, че пълното или частично разрушаване или унищожаване на енергийните критични инфраструктури може да доведе до значителни загуби за населението, икономиката, околната среда.

IV. ЗАКЛЮЧЕНИЕ

Енергия не може да се доставя без технологии и инфраструктури. Защитата на националните интереси в областта на критичните инфраструктури изисква координираност от страна на всички дружества и заинтересовани ведомства на базата на взаимен интерес, разумно разпределяне на рисковете и ефективно изразходване на финансовите средства. Състоянието на ключовите критични енергийни инфраструктури и енергийните обекти трябва да е стабилно и насочено към изпълнение на основните им задачи за качествено и сигурно задоволяване на потребностите на обществото и гарантиране на националната сигурност.

ДЪРЖАВА И СИГУРНОСТ

ХРАНИТЕЛНИ ДОБАВКИ И СИГУРНОСТ

Маргарита Бонева

FOOD'S SUPPLEMENTS AND SECURITY

Margarita Boneva

ABSTRACT: This paper presents problems of and security.

KEY WORDS: security, food's supplements, food.

Проблемите с храните и хранителните добавки в съвременното общество са особено актуални.

Научните изследванията върху храните, които употребява съвременното общество сочат, че новите технологии в областта на храненето водят до снижаване на тяхната реална хранителна стойност и до редица странични, неблагоприятни ефекти върху здравето. Индустриализацията е пряко свързана с така наречените „болести на цивилизацията“. Представата, че допуснатата на пазара и в лъскава опаковка храна е добра, е резултат на огромна обществена манипулация, извършвана от хранителния бизнес.

В индустриалнопроизвежданите или т. нар. преработени храни се добавят хранителни добавки багрила, избелващи вещества, емулгатори, антиоксиданти, консерванти, ароматизатори, буфери, подкислители, алкализиращи вещества, овлажнители, изсушаващи агенти, газове, набухватели, омекотители, дезинфектанти, дефолианти, фунгицидни средства, неутрализатори, подсладители, препарати против втвърдяване, против образуване на пяна и др. Хранителните консерванти представляват натурални или синтетични химикали, които се добавят към храна или към фармацевтични продукти – за увеличаване срока им на годност – независимо дали става въпрос за микробиологичен процес, или различни химични промени.

Точният им брой не е известен, но е изчислено, че съществуват над 7000 химически добавки, които се използват в хранително-вкусовата промишленост. Всеобщата им употреба в големи количества може да доведе до субклинично отравяне, което е толкова коварно, че лекарите не биха могли лесно да направят връзка между отровата и болестното състояние. Доказано е, че химическите добавки са свързани с редица заболявания – от алергия до рак. Инвазията на хранителни добавки в храната на глобализирания човек е емблематична. Хранителните добавки са вещества с изкуствен или естествен произход, които обикновено не се използват самостоятелно като храна или като преобладаваща съставка при производство на

храни, независимо от това дали имат хранителни свойства. Добавят се по технологични съображения към храната при производството, обработката, опаковането, транспорта или съхранението й и остават като нейна съставка, дори и в променена форма. Те се употребяват по следните технологични причини:

- Да съхранят хранителния продукт и да удължават неговия срок на годност – т. нар. консерванти.
- Да придадат или засилят цвета на хранителния продукт – оцветители.
- Да придадат или засилят сладкия вкус на храната – подсладители.
- Да подобрят вкуса на хранителните продукти – овкусители и киселинни регулатори.
- Да подобрят структурата на хранителния продукт – стабилизатори, емулгатори, сгъстители.

За класификацията на хранителните добавки и едновременно с това за осведомяване на потребителите в Европа е въведена система за класификация на хранителните добавки.

Оцветители на храни са всички субстанции, които се прибавят към храната, за да променят или подсилят нейния естествен цвят. Те могат да бъдат естествени или синтетични, извлечени от растения, билки или насекоми. Докато някои от тях са безопасни за повечето хора, малка част други могат да предизвикат нежелани реакции при някои хора. Производителите използват тези добавки, за да се свърже цвета с вкуса, който се предполага, че има храната. Тези оцветители се използват навсякъде - от винено червените дъвки до червеното вино. Въпреки, че хранителните наредби във Великобритания, ЕС и Австралия допускат употребата на тези оцветители и ги смятат за безопасни, има една малка част, която смята, че ефекта от оцветителите все още не е добре изследван и че тяхната употреба крие неизвестен риск. Американското FDA получава компенсации за всеки фунт (0,453кг.) оцветена храна, която сертифицира, което мнозина смятат за конфликт на интереси, що се отнася до безопасността на тези оцветители. Разнообразието от оцветяване на хранителните продукти и ефекта от производството и съхранението им, често прави оцветяването комерсиално, за да бъде достигнат желания от потребителя цвят. Основните причини включват:

- Загуба на цвят поради липса или прекомерна светлина, кислород, разлика в температурата, влага и условия на съхранение.
- Прикриване на природни изменения в цвета.
- Подчертаване на естествените цветове.
- Осигуряване на идентичност на храната.
- Предпазване на вкусовите данни и витамините при досег със светлина.

Хранителните оцветители се разделят на естествени и синтетични. Някои от тях са съвсем натурални, като например карамела, който е част от газираните напитки на Кока - Кола, който се добива от карамелизирана захар. Chlorella е зелена и се извлича от алгае (algae), ярко червеното багрилно вещество (Cochineal), се извлича от насекоми и се използва дори в козметиката. Някои цветове се извличат от растения и билки като захарното цвекло, куркумата, шафрана и червения пипер. Голяма част от оцветителите са забранени за употреба в хранителните продукти поради съображения за безопасност. Все още обаче има разрешени оцветители, което притеснява потребителите. Смята се, че голяма част от изкуствените оцвети-

тели в хранителните продукти, причиняват най различни реакции – от склонност към депресия до астматични симптоми при по-чувствителните индивиди - особено при децата. В Норвегия е забранена употребата на всички видове катрани (каменовъглени смоли) и неговите производни. Консервантите са вещества, използвани широко в хранителната, козметичната, фармацевтичната, дървообработващата и др. промишлеността, които служат за предотвратяване и намаляване на разграждането и/или развалянето на продукта в следствие микробно развитие и/или нежелани химични промени. Още в древни времена хората са използвали консерванти за да подсигурят дълготрайност на хранителни продукти от животински и растителен произход. Първоначално са се използвали каменна сол, мед, вино, по-късно винен оцет и алкохол. Освен за съхраняване на храни, древните хора са мумифицирали своите фараони, царе и вождове, като при този процес са се използвали мед, восък, нефт и ароматни растения. През XIX и XX век химическите консерванти от природен и синтетичен произход получават много широко приложение в хранителната, козметичната и фармацевтична промишленност. Първоначално се използвали серниста киселина, салицилова киселина, бензоена киселина и техните соли. В средата и особено в края на XX век, с цел оптимизация на положителното действие на консервантите, за всяка група продукти са разработени специални балансирани смеси от консерванти (E200-E299), обезпечаващи универсалното им приложение. Широкото им приложение е ограничено в края на века, като в някои страни определени консерванти са забранени или ограничени от здравните министерства. Наличието на тези консерванти трябва да бъде изрично упоменато върху етикета на всеки артикул. Още от древни времена хората са се опитвали да удължат срока на храната – необходимост, породила се от нуждата за оцеляване. Плодове, зеленчуци, месо и риба били изсушавани и по този начин запазвани от разваляне. Сол, захар, киселина, подправки и пушек също били използвани като консерванти. Много рано хората открили, че подсирването е ефективен начин за запазване на млечните продукти, гроздовият сок може да ферментира и да се превърне във вино, а зеле и различни зеленчуци – в туршии. Днес, въпреки че все още се използват, тези методи за запазване на хранителните продукти се оказват недостатъчни за целите на съвременната хранителна индустрия. Точно тук в действие влизат Е номерата от 200 до 299 или т.нар. консерванти. Влагането им се е превърнало във важно средство за запазване на характеристиките, външния вид на храните, както и за увеличаване на техния срок на годност. Консервантите действат като антимикробни агенти, антиоксиданти или комплексно. Те спират развитието или убиват бактерии, мухъл, плесен, инсекти или други микроорганизми в храните. Антимикробните агенти препятстват развитието на мухъл, дрожди и бактерии, а антиоксидантите предпазват храните от гранясване и поява на тъмни петна като подтискат естествените процеси, случващи се в храните при контакт с кислород, топлина и някои метали. Повечето от консервантите са химикали, които в естествено състояние се срещат в някои продукти - сорбиновата киселина (E200) може да се извлече от Самодивско дърво, натриев бензоат (E211) се открива в състава на ябълки, червени боровинки, сливи, карамфил и канела, низин (E234) в естествено състояние се открива в млякото и сиренето чедар. Много по-лесно и евтино обаче е тези консерванти да се синтезират по химичен път. Най-използвани консерванти са сорбинова киселина (Sorbic acid) (E200) и нейните соли – калиев сорбат (E202) и калциев сорбат (E203) – антимикробни агенти, използвани за предпазване на храните и

напитките от развитието на мухъл, дрожди и плесени. Списъкът с храните и напитките, в които се влагат тези консерванти е изключително разнороден – от плодови сокове и концентрати, безалкохолни напитки, сухи плодове, млечни продукти, сладоледи, сирена, туршии до вино, колбаси, месни полуфабрикати и печива. Причината е, че сорбиновата киселина и нейните соли нямат вкус и мирис, и вложени в допустимите количества се считат за безопасни. Е202 (калиев сорбат) е известен още като стабилизатор за вино - прибавя се когато активната ферментация е приключила и виното е преточено, за да убие всички останали дрожди, елиминирайки възможността за протичане на по-нататъшна ферментация. Именно Е202 се използва и за „пресичане“ на туршиите. Освен в храните калиев сорбат се прибавя и в билковите хранителни добавки като консервант. В козметичните продукти и тези за лична хигиена (кремове, лосиони, шампоани, душ гелове) Е202 се използва като заместител на парабените. Бензоена киселина (Е210) и нейните соли – натриев (Е211), калиев (Е212) и калциев (Е213) бензоат се използват за предотвратяване развитието на бактерии, дрожди и плесени в киселинни храни и напитки като плодови сокове, пюрета, концентрати, безалкохолни напитки, кетчуп, оцет, салатни дресинги. В комбинация с витамин С (Е300) бензоатите могат да образуват бензен, който е известен канцероген. Серен диоксид (Е220) и сулфити (Е221 до Е228) са консерванти, които имат мултифункционално действие и служат още като антиоксиданти и стабилизатори на цвета. Освен това имат много силно изразен антибактериален ефект. Използват се в продукти като пакетирани супи, чипс, сухи плодове и зеленчуци, плодови сокове и сладка, салами и месни продукти. Серният диоксид е важна съставка при производството на вино и бира, а натриевият сулфит (Е221) се използва за стерилизиране на оборудването при производството на вино и бира, предпазване на храните от развитие на микроби и предотвратяване обезцветяването на месо, белени картофи и ябълки. Нитрити (Е249 и Е250) и нитрати (Е251 и Е252) се използват главно в месни продукти като ги предпазват от развитието на Клостридиум ботулинум – бактерията, причиняваща ботулизъм. Освен това нитратите и нитритите стабилизират и дори правят по-наситен и привлекателен цвета на месото. Селитра (калиев нитрат) се е използвала още през Средновековието при приготвянето на различни видове осолени меса. Нитратите и нитритите дават характерния червеникав оттенък на саламите. При определени условия обаче тези съединения могат да образуват нитрозамини, които се свързват с хемоглобина в кръвта и го увреждат. Понякога, за да се неутрализират вредните свойства на нитратите и нитритите, се прибавя витамин С или Е, които предотвратяват образуването на нитрозамини, но все пак е по-добре да се избягват. Пропионова киселина (Е280) и нейните соли (Е281 – Е283) се влагат главно в печива и хлебни изделия. Предотвратяват появата на зелена плесен по хляба. Някои от хранителните добавки имат изключително вредно действие и храни, които ги съдържат трябва да се избягват. Такива са хранителните добавки:

- от Е210 до Е213 – групата на бензоатите. При определени условия е възможно да образуват карцерогенни съединения;
- от Е214 до Е219 – парабени – повечето са забранени за употреба;
- от Е220 до Е228 – групата на сулфитите. Те са алергени, разрушават витамин В1, може да предизвикат астматични пристъпи и затруднения в метаболизма при хора с нарушена бъбречна функция;

- Е236 – мравчена киселина. Тестовете с животни показват, че Е236 действа като мутаген. При честа употреба на храни, в които има мравчена киселина са възможни увреждания на черния дроб и бъбреците;
- Е249 – Е251- нитрити и нитрати – използват се главно в месните продукти. Това са потенциални карцерогени и са забранени за употреба в храни за бебета и деца.

След като компаниите-производители представят добавките пред хранителната индустрия, правителството е длъжно да вземе мерки и е задължено да проверява дали тези добавки са безопасни за здравето на хората. Въпреки това, някои консерванти са забранени за употреба, години след като са били разрешени, тъй като с времето технологията за тестване на продуктите става по-прецизна и точна. Ето защо, хората смятат консервантите за изключително вредни. Науката продължава да работи по въпроса, да произвежда нови добавки, да подобрява методите за тестване на продуктите и да прави промени. Развитието на технологиите също помага много в процеса на проверка на безопасността на продуктите. Законодателството в тази област също се обновява непрекъснато, за да бъде в крак с новите технологии за производство. Хранителните добавки сами по себе си не са нещо "лошо". Например: ascorbic acid съответства на витамин С, а alpha-tocopherol е всъщност витамин Е. Антиоксидантите предпазват храната от бързо разваляне, променят вкуса и възстановяват цвета, загубен при обработка на продукта. Витамини С и Е се използват именно като антиоксиданти. Емулгаторите се използват, за да поддържат смес между вода и мазнина. Лецитинът, например се използва при производството на маргарин, печива, сладолед. Моно и ди- глицеридите са други добавки, които се срещат в подобни хранителни продукти, както и във фъстъченото масло. Polysorbate 60 и 80 се употребяват в кафето, и като състав на изкуствено произведената сметана. Сгъстителите абсорбират водата и запазват смесени мазнините, водата, киселините и твърдата храна. Alginate се добива от морски водорасли и се употребява, за да се подобри качествения строеж на сладоледа, сиренето и млякото. Casein (казеинът) е млечен протеин, който се употребява в производството на сладолед, шербет и сметана за кафе. Някои от добавките предизвикват алергии, други водят до диабет, трети дразнят стомаха, четвърти влияят зле на функциите на мозъка, а една голяма част са доказано канцерогенни – тоест, причиняват рак. Тези добавки, за които никой не ни разказва в етикетите и не ни предупреждава за страничните им действия, са най-опасни за децата, още повече, че се съдържат в газирани и подсладени напитки, дъвки, сладкарски изделия и други лакомства, които им купуваме всеки ден. Преди повече от 100 години в началото на миналия век понятието хранителна добавка било твърде условно, а контролът върху използването им – още по-условен. В разхладителните напитки например напълно законно добавяли кокаин, а едно от патентованите лекарства против кашлица бил хероинът. През 60-те години на миналия век в Тайланд специалисти във фирма за производство на детско лекарство вместо предвидения по технология пълнител пропиленгликол, добавили аналогичния по физико-химични свойства, но доста по-евтин етиленгликол, който обаче се използва като основен компонент на охлаждащата течност на автомобилите. В резултат на това 300 деца починали от токсична некроза на черния дроб, а няколко хиляди получили тежки отравяния.

По същото време смятали метамфетамина за безвреден стимулатор. Едва след като в продължение на 5 години широко го използвали, лекарите и пациентите

научили за смъртоносните странични ефекти на този препарат, който сега е в групата на т.нар. тежки наркотици. Европейските правила за регистрация на биологически активни вещества, или иначе казано добавки в храните, са доста строги. Международните изследователски центрове по поръчка на Европейския съюз стриктно проверяват безопасността им. На практика обаче една и съща фирма може да произвежда дадена храна за вътрешно потребление, за износ в развити страни с контрол върху добавките, и за износ в развиващи се страни. Така и в нашата страна съвсем редовно могат да попаднат храни, не само екологично опасни, но и произведени с опасни за здравето консерванти. Много често върху етикета почтено на пръв поглед е вписан въпросният консервант, но със съответния му Е-номер. Така производителят ни е предупредил, а ние като купувачи ще трябва да решите ще закупите ли опасната храна, която по правило е по-евтина, или ще предпочетем по-скъпата, но по-качествена и безвредна стока. Символът Е с различните номера, с които се обозначават добавките в храните, означава стандартите на Европейския съюз. Същите цифри без обозначение Е са разрешени във Великобритания, а САЩ използват друга система на класификация. От Е 100 до Е 181 е групата на оцветителите. Използват се в сладки газирани напитки, лимонади, бонбони, близалки, сладолед. От Е 200 до Е 290 са консервантите и ги намираме във всички консервирани храни - гъби, компоти, сокове, конфитюри и сладка. От Е 296 до Е 385 са киселини и антиоксиданти. Те предпазват продуктите от разлагане и се откриват в млечно-кисели продукти – подсладени плодови млека, десерти, салами, краве масло, шоколад. От Е 400 до Е 495 са гуми, емулгатори, стабилизатори и сгъстители, които запазват консистенцията на продукта. Използват се в сладка, конфитюри, желета, кондензирани млека, шоколадови десерти, млечни продукти. От Е 500 до Е 585 са минерални соли. От Е 620 до Е 640 са овкусители, ароматизатори и подобрители. От Е 900 до Е 999 са пенорегулатори и се използват в газираните напитки. Добавките от Е 1000 до Е 1199 помагат продуктите да не попиват влага и се добавят към брашното, захарта и други подобни продукти. От 81 оцветители, 20 са забранени. Абсолютно забранени са два от тях: Е 121 – цитрусов червен оцветител, и Е 123 – оцветител амарант, който се използва в миксове за кекс, плодови пълнежи и желета и предизвиква астма, екзема, хиперактивност и е вреден при бременност. Е 102 е тартазин. Той се използва в безалкохолни напитки, сладкиши, снаксове, тестени храни, консервирана риба, готови супи. Предизвиква астматични пристъпи и алергия при децата и е забранен в Норвегия и Австрия. Следващият Е 104 се използва в червила, козметика за коса, причинява дерматит и е забранен в САЩ, Австралия и Норвегия. Е 133 се използва в млечните продукти, сладка и напитки и е забранен в 7 европейски държави. Е 142 е дериват от въглищния катран, използва се при консервирания грах и е забранен в Швеция, САЩ и Норвегия. Друг подобен дериват на въглищния катран, Е 151 е забранен в 9 европейски държави и САЩ. Списъкът е много дълъг. Оцветителите с номера Е103, Е105, Е121, Е123, Е125, Е126, Е130, Е131, Е142, Е152 и Е153, консервантите с номера Е210, Е211, от Е213 до Е217 и Е240, който е формалдехид, антиоксидантът Е 330, Е 447, Е924 А и Б са канцерогенни. Черният дроб и бъбреците могат да увредят добавките от Е171 до Е173, Е320 и Е322, Е407, Е447 и Е450. Нарушават функциите на кожата добавките от Е230 до Е233. Противопоказни при хипертония са от Е250 до Е252. Алергии предизвикват добавките с номера от Е230 до Е232, Е239 и антиоксидантите от Е311 до Е313.

По щандовете на магазините се срещат често храни с по 3, 4 и дори 6 вредни добавки. Такива са например пакетчетата ролца от раци, които съдържат 4 добавки, 2 от които вредни: изкуственият подсладител сорбитол под символа Е 420, който не е разрешен за детски храни и може да предизвика стомашни смущения, и алергенният Е 621. Във всяко пакетче готова суха пилешка супа например, се съдържа също алергенният Е 621, както и предизвикващият подагра Е 627. Любимите на всички деца дъвки пък са сред най-опасните, защото съдържат най-вредната добавка – Е 951, наречена аспартам. От сладкишите пък се дебелее не само заради захарта. Оказва се, че те масово съдържат 2 добавки: Е 233, предизвикваща кожни проблемиР и Е 435, като и двете водят до затлъстяване. Често срещаният в натуралните сокове червен оцветител Е 122 предизвиква алергии и астматични пристъпи. Колбасите също съдържат доста вредни съставки. Най-често това е Е 250 – натриев нитрит – канцерогенен и забранен в много страни. Среща се както в трайните салами, така и в лионската наденица и пилешките кренвирши. Особено рискови са сосовете и подправките, с които консумираме месата и надениците. Те съдържат забранения оцветител Е 110, който предизвиква обриви, отоци, повръщане и който се използва и в сухите супи и сладкишите. В шоколадовите изделия пък често се среща Е 553b или талк, който причинява рак на стомаха. Така се оказва, че най-много рискови добавки има в дъвките, сосовете, месните и сладкарски изделия и особено в безалкохолните напитки.

Мит се оказва и славата на антиоксидантите като много полезни. Витамин С над препоръчителната доза от 60 милиграма дневно е опасен, защото ускорява стесняването на артериите и уврежда сърцето. Витамин А, наречен още ретинол, който е известен и като витаминът на растежа, според изследване на Националния институт по рака в САЩ при употреба увеличава риска от рак на белия дроб и на простатата. Селенът в големи дози е много токсичен. В китайските ресторанти в САЩ първи започнали да използват натриев глутамат. След известно време общността започнала да забелязва връзката между главоболие, подуване на стомаха, припадъци и други оплаквания с китайските ресторанти. Нарекли явлението Китайски синдром. Впоследствие се оказало, че това се причинява от натриевия глутамат. Практически цялата храна в китайските ресторанти е богата на това вещество. То се съдържа в особено големи количества в морските деликатеси. Означава се като Е 621. Той обаче е един от най-тежките разрушители на мозъка, отдавна забранен в Швеция. Изключително опасна добавка е Е 951 или аспартам. Това е изкуствен подсладител, повече известен като нутрасуит. Изключително широко се използва в газираните напитки и разтворимите прахчета. В част от продуктите дори не е отбелязан на етикетите: дъвки без захар, какаови смеси, напитки с кофеин, разтворими чай и кафе, сокове, мултивитамини, сосове, бързи закуски. Документирани са 92 симптома, причинявани от аспартама: вцепеняване, главоболие, умора, световъртеж, гадене, сърцебиене, затлъстяване, неразположение, раздразнителност, безспокойство, амнезия, замъглено зрение, обриви, удар, ослепяване, ставни болки, депресия, спазми, спонтанни аборти, безплодие, пристрастяване, слабост и загуба на слух. Аспартамът отключва и някои други болести: мозъчни тумори, множествена склероза, епилепсия, хронична умора, паркинсонова болест, алцхаймер, диабет, дефекти при раждането. Страничните му действия са още по-опасни, защото по-голямата употреба води до пристрастяване. Много хора съобщават за тежък абстинентен синдром, когато се опитат да изхвърлят аспартама от

храната си. Някои твърдят, че предизвиква дори по-силна зависимост от алкохола. Причинява 75% от страничните реакции от всички добавки. Изследванията на действието на много от тези хранителни добавки все още продължава. Основното правило в нашето законодателство е да не се превишават смятаните за безопасни дози от тези вещества.E249 Potassium nitrite (Калиев нитрит) е фиксатор/стабилизатор на цвета и консервиращ агент за месо. Нитритите могат да засегнат способността на тялото да пренася/усвоява кислорода и в резултат на това да причинят недостиг на въздух/задушаване, замайване и главоболие. Забранен в храните за пеленачета и деца. Потенциален канцероген е E250 - Sodium nitrite (Натриев нитрит). Може да се свързва с химикали в стомаха, образувайки нитрозамин, както и да предизвика хиперактивност и други вредни реакции. E252 - (Калиев нитрат). Може да причини хиперактивност и други вредни реакции. Потенциален канцероген. Забранен в много страни. E261 - Potassium acetate (Калиев ацетат). Добавя се в сосове и туршии. Да се избягва от хора с нарушена бъбречна функция. E264 - Amonium acetate Амониев ацетат. Може да предизвика гадене и повръщане. E281 - Sodium propionate Може да доведе до мигрена. В списъка на опасните консерванти са: E102, E124, E120, E127, E123, E103, E111, E105, E121, E125, E130, E126, E152, E104, E141, E122, E150, E171, E173, E180, E241, E477, E131,E210,E142,E211,E212,E 215, E213, E216, E217, E330, E240, E221, E223, E-22, E224, E226, E230, E238, E231, E311, E313, E312, E250, E251, E-230, E321, E322, E338, E340, E339, E341, E407, E461, E450, E462, E463, E466, E465.

Строгият контрол върху хранителните добавки и тяхното познаване от всеки гражданин гарантира здравето на населението. Намаленият и сведеният до минимум здравен риск в резултат на това е гаранция за националната сигурност на всеки народ.

ЛИТЕРАТУРА

1. Эмануэль Н. М., Лясковская Ю. Н., Торможение процессов окисления жиров, М., 1961.

2. Эмануэль Н. М., Денисов Е. Т., Майзус З. К., Цепные реакции окисления углеводородов в жидкой фазе, М., 1965.

3. Ингольд К., Ингибирование автоокисления органических соединений в жидкой фазе, пер. с англ., «Успехи химии», 1964, т, 33, в. 9.

4. Оковитый С. В., (2009), Клиническая фармакология антиоксидантов, М., с.602

ТОКСИЧНИ МЕТАЛИ

Маргарита Бонева

TOXIC METALS

Margarita Boneva

ABSTRACT: This paper presents problems of toxic metals.

KEY WORDS: security, ecology, toxic metals.

През втората половина на XX век се наблюдават значителни промени в хранението и стила на живот, които допринасят за епидемия от неинфекциозни заболявания като сърдечно-съдови болести, някои ракови заболявания, диабет тип 2, затлъстяване, остеопороза, кариес.

Попадането на биологични, химични и радиоактивни замърсители в храните създава потенциален риск за здравето на потребителите. Замърсителите на храните могат да окажат непосредствен ефект (остри хранителни инфекции и интоксикации) или да имат хронично токсично въздействие и отдалечен здравен ефект (мутагенност, канцерогенност, влияние върху репродукцията, тератогенност и ембриотоксичност, алергенност). В храните попадат потенциално опасни за здравето вещества, в резултат на замърсяването на околната среда от индустрията и траспорта, както и от неспазване на условията на добрата селскостопанска и производствена практика: тежки метали (олово, кадмий, живак), арсен, пестицидни остатъци, нитрати, микотоксини

Групата на тежките метали обхваща 2/3 от Периодичната система на химичните елементи. Токсичните тежки метали в по-голямата си част са катиони, лесно натрупващи се в почвата и бавно отделящи се от нея. По решение на ЮНЕСКО това са: живак (Hg), кадмий (Cd), олово (Pb), ванадий (V), кобалт (Co), манган (Mn), мед (Cu), никел (Ni), калай (Sn), стронций (Sr), цинк (Zn) и титан (Ti). По степен на токсичност тежките метали се групират в три групи:

В първа група са живак (Hg), кадмий (Cd), олово (Pb), арсен (As), селен (Se), цинк (Zn), титан (TI), втора група- кобалт (Co), никел (Ni), молибден (Mo), мед (Cu), хром (Cr) и трета група- барий (Ba), ванадий (V), манган (Mn), стронций (Sr), алуминий (Al). Най-опасни за човека са металите от първата група.

Още в древноегипетските папируси са споменати различни отровни растителни и химически вещества, между които токсичните метали: олово, живак, арсен и мед.

Годишно в атмосферата постъпват около 2000 мил. тона естествен аерозол, съдържащ токсични метали и техни съединения. Металите попадат във въздуха във вид на малки частици, образуващи се при изгаряне на въглища, нефт, производство на стомана или сплави на цветни метали. По тази причина в земната атмосфера метали като: злато, кадмий, олово, селен, телур са хиляди пъти повече, отколкото е било при естествени условия. Дисперсни частици от метали могат да се внесат в атмосферата и при изригване на вулкани, при земетресения, при изпарения на водни разтвори.

Оловото е отдавна известна отрова. Още в древен Рим са били известни оловни тръби за водопроводи и оловни сплави за кухненска посуда и съдове за вино. Химическото откриване на олово в останки, запазени от древни римляни показват това, че в техния организъм е имало твърде много от този метал. Може би в това се крие една от причините за упадъка на могъщата древна империя. Счита се, че сега в Балтийско море ежегодно постъпват повече от 5000 тона олово, при което ¾ от това количество попада в морето от въздуха. Забележимо е присъствието на олово даже в ледовете на Гренландия.

Тежките метали и техните соли постъпват във водоемите от естествените източници – подземни рудни пластове, повърхностни слоеве на почвата и подземната вода, изтичащите води на много фирми, атмосфени утайки, които замърсяват от димовите изхвърляния. Под действие на живи организми във водоемите – микроби, живакът, оловото, арсенът се подлагат на метилиране и се превръщат в по-силно токсични алкилни съединения. Живакът, оловото, кадмият, арсенът, цинкът постъпват в човешкия организъм чрез храната и могат да предизвикат интоксикации.

Източници на замърсяване на почвата с токсични метали са отпадъци от металообработващата промишленост, продукти от изгарянето на топливо, автомобилни отпадъци, поливане на земеделски култури с отпадни води, използване на шлаката за тор, която е богата на тежки метали. Съдържанието на кадмий достига 275 мг/кг, оловото е в същото количество, по-малки са количествата живак и други тежки метали.

Металообработващите фирми ежегодно изхвърлят на повърхността на земята огромни количества метали – олово, мед, цинк, молибден, живак, кадмий.

В райони по-богати на никел в почвите и водите населението има повишена заболеваемост на роговицата на окото.

При повишено съдържание на стронций в почви, води и растения се наблюдава размекване на костите от скелета на животните, т. нар. „стронциев рахит“, който не се поддава на лечение нито с витамин D, нито с калций и фосфор.

С растителната храна в организма постъпват 75-80% от основното количество тежки метали. В растения, отглеждани около пътни магистрали е доказано повишено съдържание на олово, цинк, никел и кадмий.

Установено е, че най-голямо количество олово и кадмий се приема чрез храната – растителна и животинска.

Прекомерната експозиция на кадмий може да доведе до бъбречнотубуларно увреждане и до обструктивна белодробна болест.

Една от най-страшните болести сред възрастните – болестта на Алцхаймер, се дължи на вредното влияние на алуминия, тъй като при аутопсия на починали от това заболяване са намерени по-големи алуминиеви концентрации в мозъка.

Неврологични промени може да предизвика и магнезият, като засяга предимно пирамидните пътища.

Синдромът „внезапна смърт на кърмачетата“ се дължи на хистаминов шок, който както е известно се причинява от недоимък на магнезий. В райони, в които питейната вода съдържа недостатъчно количество магнезий, се наблюдава внезапна смърт от остра сърдечна недостатъчност.

Установено е, че токсичността на тежките метали се дължи на свързването им със сяросъдържащите вещества на ензимите и белтъците. Особена роля има нискомолекулярният белтък металотионин, който се съдържа в 61 или 63 аминокиселини.

Живакът предизвиква увреждане на мозъка, визуална, сензорна, слухова и координационна дисфункция, тремори. Оловото е причина за енцефалит, смущения в поведението, интелектуален дефицит, намален контрол на нервите.

Талият води до енцефалит, мозъчни тумори, полиневрит.

Арсенът е причина за вертиго, безпокойство, раздразнителност, загуба на слуха, моторна парализа, периферен неврит.

Бисмутът предизвиква периферен неврит, селенът – депресия и раздразнителност, а телурът води до тремори, намалени рефлексии, конвулсии.

Увреждане на здравето от алуминий се констатира само при масивна експозиция. Отдавна е известен „албуминов бял дроб“ при работници в среда с фин алуминиев прах, при което се наблюдават необратими промени в дихателните пътища и белите дробове, водещи до белодробна фиброза. Прогресивна енцефалопатия е описана при работещи на пещи за топене на алуминий

При остри интоксикации с арсен се наблюдават силни болки в корема, обща слабост, повръщане, диария, главоболие, главозамайване, перфорация на стомаха и червата. В някои случаи се наблюдава депресия, вцепененост, парализа на крайниците, шок, кома. Хроничното отравяне с арсен води до поява на пигментация, възпаление на венците, язви по устата и носната лигавица, възпаление на конюктивите. Развива се хиперхромна, перниciозо подобна анемия, симетрични полиневрити, напредващи центропентално, мускулна слабост, последвана от мускулна атрофия. Арсенов прах може да предизвика кожен рак или появата на бронхиален рак.

При краткотрайни експозиции с високи дози живачни пари се увреждат белите дробове. Клиничните прояви са болки в гърдите, кашлица, диспнея, остра дихателна недостатъчност. При продължителна експозиция на живачни пари критичен орган е мозъкът. Основни симптоми са слабост, умора, сънливост, апатия, главоболие, световъртеж, живачен тремор, промени в психиката – повишена възбудимост или потиснатост, разстройство в паметта, чувство на страх, загуба на самоконтрол, склонност към плач, маниакално депресивна психоза. Вегетативни смущения – хиперсаливация, хиперхидроза, тахикардия, брадикардия, дермографизъм, полиурия. От страна на периферната нервна система се наблюдават – невралгии, неврити и полиневрити. Критични органи са мозъкът, бъбреците и стомашно-чревния тракт.

Един от най-токсичните елементи е кадмият. Той уврежда клетките, произвеждащи еритропоетин в бъбреците. Води до повишаване на кръвното налягане. Кадмият е канцероген. Предизвиква остри и хронични интоксикации, белодробни тумори, рак на простата у мъжете, бъбречно тубуларна дисфункция, скелетни проблеми, ниско тегло на новородените, увреждa белите дробове и всички паренхимни органи - далак, черен дроб, щитовидна жлеза, надбъбреци, бъбреци, тестиси, костна система.

При високи концентрации на меден прах в белите дробове се наблюдава „медна треска“ с ерозии на белите дробове, катар на горните дихателни пътища и тежък астматичен бронхит, зачервяване на чревната лигавица, повърхностни некрози, остра бъбречна недостатъчност, анемия, хемолитичен шок и мозъчни увреждания, бъбречна недостатъчност, грануломи, туморни образувания. Развива се болест на Уилсон, характерна с отлагане на мед в черния дроб и мозъка.

Никелът е силен канцероген. Предизвиква екземи и язви, церебрален, белодробен и кожен синдром, протичащи съответно - с умора, главоболие, безсъние, с

хроничен катар на горните дихателни пътища, астматичен бронхит, белодробен рак, с развитие на хронични алергични дерматози и екземи.

При отравяния с олово се наблюдават невропатии, хипохромна анемия, увреждане на стомашно-чревния тракт, бъбреците, черния дроб, сърдечно-съдовата система – ранна атеросклероза с цереброваскуларни промени, токсичен миокардит. Увреждане на ретината и на зрителния нерв, което може да доведе до ослепяване.

Хромът и неговите съединения се натрупват в белите дробове, черния дроб, слезката, панкреаса и костния мозък. Този метал стимулира синтезата на холестерола, с което се свързва ранно развиващата се атеросклероза при експонираните лица. Има канцерогенен и алергичен ефект. При остра интоксикация бързо се развива тежък трахеобронхит и хромови пневмонии до развитие на белодробен оток. Наблюдава се развитие на токсична нефропатия. Постъпването на хромови съединения в храносмилателния тракт протича с дискинезии, гастрит с чести обостряния и повишена киселинност. В различна степен се уврежда черния дроб и бъбреците.

Цинкови пари предизвикват леярска треска (цинкова треска). Може да се увредят и гастротестиналните пътища, появяват се язви на стомаха и дванадесетопръстника. Регистрирани са развитие на хипохлорна анемия, пневмосклероза, атеросклероза, нарушена сърдечна дейност, хипогликемия, анемия, хиперхолестеренемия.

Отравянията с барий водят до миниероподобна симптоматика – загуба на равновесие, нарушение на говора, зрението, слуха, парализи, биоаритимия, хипертония, миокардна и цялостна мускулна стимулация, кръвоизливи в стомаха, дванадесетопръстника и лявата камера на сърцето, масивен белодробен оток, катарални изменения на дихателната система и храносмилателния тракт.

Отравянията с ванадий водят до кожни увреждания, белодробни проблеми, главоболие, виене на свят, тремор на крайниците, нарушения на зрението, нервно-психични признаци, токсичен хепатит, токсична нефропатия.

Интоксикацията с манган и негови съединения води до манганови пневмонии, увреждане на стомашно-чревния тракт, главоболие, виене на свят, лесна уморяемост, отпадналост, парастезии на горните крайници, полова слабост, безапетитие, Паркинсонов синдром, увреждане на черния дроб и бъбреците.

Селенът е елемент с едновременно токсично и есенциално действие. Интоксикацията със селен води до намаляване на артериалното налягане, стомашно-чревни разстройства, развитие на белодробен оток, нарушения на ЦНС. Възможно е развитие на токсична и чернодробна кома, увреждане на бъбреците и миокарда, бронхопневмония, вторична анемия, контактен дерматит.

Постоянното постъпване на токсични метали в организма на човека е опасно за здравето му. Във връзка с такива техни биологични особености, като кумулация в организма, наличие на продължителност на биологичен полуживот, възможности за мутагенно, канцерогенно, тератогенно, ембрио- и гонадотоксикологично действие проблемът придобива особено значение.

В много случаи замърсяването на хранителни суровини с токсични метали има техногенен характер. Тежките метали постъпват в околната среда във вид на елементи, органични и неорганични съединения. В хранителните продукти, богати на белтък, голяма част от металите реагират с метионина и образуват белтъчни комплекси. В растителните продукти токсичните метали се съдържат в йонна форма или свързани предимно с растителен белтък или пектин.

Особено важно за здравето на човека е провеждането на непрекъснат мониторинг на хранителните продукти, водата, почвата и въздуха за съдържание на тежки метали.

Необходимо е да се проведат множество агрохимични и ветеринарни мероприятия, насочени към очистване на почвата, подбиране на адекватни торове, селскостопански култури, храни и пасища за животните. Установяването на фоновите нива за съдържание на токсични метали в хранителните продукти, получени от всяка територия и източниците на замърсяване е особено важно.

Основен път за намаляване на съдържанието на токсични метали в продоволствените суровини е използването на икономически оправдани и реално прилагани технологии, водещи до максимално намаляване на съдържанието на токсични метали, без промяна или максимално възможно изменение на показателите на храната и биологичните ценности на продукта. По отношение на тежките метали не трябва да се забравя, че кулинарната обработка на продуктите, както от животински, така и от растителен произход практически не променя тяхното съдържание, защото те се намират под форма на трайно съединение, здраво свързани с продукта, не се разтварят във вода и имат висока точка на кипене.

Под особен контрол за съдържание на токсични метали трябва да бъдат детските консервирани храни и посудата за приготвяне и консервиране на хранителни продукти. Строго трябва да се контролира съдържанието на тези елементи в различните видове хранителни добавки.

Установяването на отношението на концентрацията на тежките метали в човека към нивата им в околната среда е основа за определяне на здравния риск. Поглъщането на тежки метали от човешкия организъм и нивата им служат за основни данни за изчисляване на доза-ефект. Въз основа на тази информация се създава мониторинг на здравните ефекти. Определянето на концентрациите на тежки метали в човешкото тяло ще позволи да се проведат съответни терапевтични мероприятия за подобряване на здравето на хората. Счита се, че най-добре е да се изследват онези органи и системи, в които се кумулира даден елемент. Например, оловото се кумулира в костите, зъбите и косата, живакът – в бъбреците и косата, кадмият – в бъбреците, арсенът в носа и ноктите.

Въпросът за замърсяването на околната среда и хранителните продукти с токсични метали е особено важен, защото здравето на хората има пряко отношение към националната сигурност на всяка държава. Известно е, че по пътя на хранителните вериги токсичните метали и техните съединения чрез почвата, водата, въздуха и растенията попадат в растенията и в организма на животните и съответно в храната от растителен и животински произход. Включени в хранителната верига те крият токсикологичен риск за здравето на хората.

В настоящия момент екологичната криза е реалност. Населението на всички страни в света е загрижено за глобалното замърсяване на околната среда. Замърсяването на селскостопанските продукти е свързано с технологичните процеси, като производство, опаковка, съхраняване, транспорт и реализация на продукцията. При производството на екологично безопасни и биологично пълноценни фитопродукти е необходимо отчитане на източниците на замърсяване и определяне на стратегията по отношение на широко управляеми замърсители, влизащи в състава на агрохимикалите и създаване на мониторинг на компонентите на ландшафта. От първа необходимост е:

- създаването на безотпадни технологии и прекратяване на постъпването на токсични метали във водата, въздуха и почвата;
- ограничаване на засаждането на някои селскостопански растения около фирми и автомагистрали, замърсяващи околната среда с токсични метали;
- забрана за производството на оловен бензин и използването му;
- модернизиране на фирмите за производство на химикали и торове;
- провеждане на мониторинг на замърсяванията на домакинствата с токсични вещества; ефективен вътрешен санитарен контрол на месо и месни продукти, мляко и млечни продукти, зеленчуци и други хранителни продукти;
- контрол върху спазването на Постановления, Наредби и Закони, свързани с борбата за опазване на околната среда, хранителните суровини и продукти;
- непрекъснато повишаване на културата на населението с оглед включаването му в борбата за създаване на екологично чиста околна среда и продукция.

Проблемът със замърсяването на околната среда с токсични метали има пряко отношение към националната сигурност, защото опазването на здравето на населението е един от жизненоноважните приоритети в Стратегията за национална сигурност. Здравето на човека е един от основните социално-екологични проблеми на сигурността, чието решаване е актуално в съвременното общество.

ЛИТЕРАТУРА

1. Boneva, M., (2008), Social ecology, V.T., Faber.
2. Boneva., M., (2012), Socialecology problems of security, V.T.
3. Slatinsky, N., (2000), Dimensions of security., S.
4. Stoianov, S., (1999), Toxic metals, S.
5. Tchvan, J., Chinkina, M., (2011), Ecology, M.

СОЦИАЛНА МАНИПУЛАЦИЯ И СИГУРНОСТ

Маргарита Бонева, Георги Колев

SOCIAL MANIPULATION AND SECURITY

Margarita Boneva, Georgy Kolev

ABSTRACT: This paper presents problems of social manipulation and security.

KEY WORDS: security, manipulation, mind, behavior.

Правото на неприкосновеност на съзнанието е едно от най-важните изисквания на 21 век, тъй като с всеки изминал ден съзнанието ни е обект на все по-интензивно и масирано проникване с цел да бъде манипулирано в полза на чужди на индивида интереси.

Натрапливата реклама и непрестанно повтарящите се пропагандни послания са грубо и безсрамно нарушение на неприкосновеността на човешкото съзнание, което при други обстоятелства е било свещено убежище на аза, но днес се е превърнало в пренаселен showroom на политически алтернативи, алкохолни и безалкохолни напитки, автомобили, дизайнерски облекла, козметика, райски плажове, конкурси за красота, възможности за инвестиране, порнография, развлечения и всякакви форми на потребление.

Телевизията не само нахлува в човешкото съзнание, но и руши спокойствието на дома, като агресивно се стреми да впечатлява.

От друга страна, психическите способности на човека са жертва на силно замърсяване на околната среда с шум и други вредни въздействия. Всичко това разсейва и отслабва съзнанието и го прави податливо на управление отвън.

Човешката психиката е обект на постоянни манипулации.

Изкуственото създаване на отчуждаващи или задължителни потребности от разкош, както и подтикването на хората чрез подмолно сублиминално проникване в психиката им да вършат несъзнателни неща, които в действителност не желаят е посегателство срещу свободата на индивида.

Манипулирането на човешкото поведение чрез средствата за масова информация с цел хората безропотно да приемат неща, които иначе биха отхвърлили, е посегателство върху човешката свобода.

В демократичните страни гражданите не са длъжни да приемат безпрекословно погрешни или незаконни решения на властниците, да търпят послушно липсата на прозрачност в решенията на съда, нито пасивно да се съгласяват да плащат прекомерни или неизвестно за какво предназначени данъци. Въпреки това въздействието на различните форми на манипулация на човешкото съзнанне се усеща пряко или косвено в цял свят. Целта на тази манипулация е гражданинът да бъде подчинен на желанията на прикрити интереси.

Демократичният принцип за „управление от народа“ се изпразва от съдържание и смисъл, тъй като съзнанието на хората е подчинено на медиите и техните ръководители, а не на самите хора.

Свободата на мисълта е нарушена в самата си основа.

Според Карл Попър „Телевизията се е превърнала в прекалено силна за демокрацията власт. Никоя демокрация не може да оцелее, ако не сложи край на злоупотребата с власт от страна на телевизията. Днес тази злоупотреба е очевидна. Злоупотребата с власт от страна на телевизията и печатните медии е форма на идеологически тероризъм срещу хората. Той трябва да бъде поставен под строг контрол от специализиран орган за наблюдение на етиката, както предлага Попър. Контролът върху съзнанието на хората в днешно време е прекрасен бизнес. Всеки, който има достатъчно пари, може да проведе рекламна кампания и да въздейства върху поведението на потребителя. Господстващите икономически системи силно се стремят към такова въздействие, защото то увеличава продажбите и води до натрупване на големи състояния.

Всеки консумира не само материални блага, но и идеи и ценности. Именно в тази област хората са подложени на непрестанно „промиване на мозъка”, чиято цел е да насочи човешкото поведение в подходяща посока според определени интереси.

Много отдавна амбициозни индивиди са открили, че господството над чуждата воля може да стане неизчерпаем източник на власт. За съжаление все още не е

намерен начин да се предпазим от това инвазивно манипулиране на човешкото поведение. Такава защита може да се постигне само със строг контрол върху човешкото съзнание.

Налице е ситуация, при която индивидът да се подчинява на мажоритарното мнение на „нейно величество тълпата“, дори когато знае, че то е уродливо, променливо, краткотрайно и не е плод на интелигентен мозък, защото тълпата няма такъв. Обикновено тълпата действа като инструмент в ръцете на амбициозни хора, които благодарение на своя престиж, чар или ораторски способности са постигнали прекомерно влияние върху масата, като истинските им подбуди остават неясни.

Политическата демагогия е открито неморално поведение, защото хората са манипулирани, за да бъдат използвани за лични цели и не служи на действителните интереси на народа.

Тълпата е обект на различни форми на ласкателство и привличане на външни сили, желаещи по някакъв начин да се възползват от силата й. В репресивните си форми техниките за овладяване на човешкото поведение стигат до небезизвестното „промиване на мозъка“. Става дума за определена форма на психологическо мъчение, което има за цел да промени драстично поведението на хората. То се състои в психическа дезориентация на жертвата, която се държи неограничено време будна или се подлага на продължителна умора, неудобство, глад или тревога.

Нови техники за промиване на мозъка се използват и днес като мирен, но не и безвреден начин да се промени поведението на индивида, било случайно, било преднамерено от външни сили. Една от случайните или „нормални“, но и най-могъщи форми на такова въздействие е съвременният начин на живот на нашата цивилизация.

Днес са налице поне два елемента на принуда, наподобяващи промиването на мозъци – дезориентацията и тревогата. Няма нищо по-дезориентиращо и стресиращо от все по-нарастващата сложност на живота в големите градове, информационния взрив, объркването на ценностите, насилието, шума, престъпността и корупцията в обществото.

Загубата на контрол над собствения разум се засилва от постоянното „промиване на мозъка”, предизвикано от дезориентацията и тревогата, които са нормален, но и противоестествен елемент в нашия живот.

Голяма част от психическите смущения и заболявания са следствие от неспособността на индивида да синтезира в съзнанието си по разбираем за него начин сложната действителност на една цивилизация.

Външните източници за влияние върху подсъзнанието се крият в рекламата и пропагандата. Известно е, че рекламата може да въздейства върху мотивацията на индивида с обещание да задоволи неговите скрити потребности. Според Ванс Пакард осем са подсъзнателните потребности, които се използват като мотивация:

- Емоционална сигурност.
- Потвърждаване на собствената стойност.
- Задоволяване на собствения „аз“.
- Творчески отдушници.
- Обекти на любов.
- Усещане за власт.
- Усещане за сигурност.
- Безсмъртие.

Това са осем изпитани начина за манипулиране на подсъзнанието без нормалните хора да могат да се предпазят от тази инвазия.

Своеобразното външно преизграждане на личността цели да се придаде възможно най-привлекателен вид на дадена личност, особено по време на избори.

Необходимостта да се спечели подкрепата на народа принуждава кандидата да стане актьор. В президентските кампании, например се предизвиква раздвижване на огромни маси, извършва се прикриване или подмяна на истинската личност на кандидата – едно преднамерено и предварително обмислено изкривяване на неговия характер и начин на съществуване. За съжаление президентите се избират не по рационални, а по емоционални причини. Мотивацията на електората е подсъзнателна, сантиментална, пристрастна.

Всъщност електоратът гласува и избира един идеален, но несъществуващ в действителност субект, едно творение на маркетинга, а не човек от кръв и плът.

По подобен начин стоят нещата при избора на депутатите и на всички висши чиновници в управлението на една страна, избирани с вота на народа.

Всички те без изключение трябва да са максимално прозрачни в поведението си, за да може народът да се увери, че изборът му е правилен. Манипулирането на масите с помощта на изграден за тази цел, но неотговарящ на истината образ, е много сериозно етично нарушение. Всъщност то е престъпление, защото се извършва колективна измама с утежняващо вината обстоятелство, че нейна жертва могат да станат хора с оскъдни средства или напълно беззащитни пред менталната манипулация индивиди. В края на XX век в обществото се наблюдава умствено и психологическо уеднаквяване на хората, които живеят под „Тиранията на масите“, който ги принизява до тягостна посредственост. „Тълпата е като безмозъчно всепоглъщащо чудовище, лишено от интелигентност и воля. В ежедневието всеки зависи от чуждото мнение до степен на превръщане на тълпата в „съдник и арбитър“ на поведението, при което се правят всякакви жертви, за да бъдем смятани от другите за себеподобни. Страхът да сме различни поради социалната санкция, която предполага различието – недоверие, оспорване, отхвърляне превръща всеки от нас в част от еднородна маса и това ни дава усещането за прием, сигурност и обич, но и за липса на самоличност, за самота и вътрешна тъга. Материалното натрупване в големите градове се превръща в „психическо натрупване“, което предизвиква тревожност поради усещането за загуба на „аза“. Това е една от причините, поради която в търсене на истинската индивидуалност, хората правят тъкмо обратното на това, което трябва. Посредствеността на хората се дължи на факта, че личността предварително се отказва да развива своята индивидуалност, защото й е по-лесно и по-приятно да се слее и изравни с тълпата, като разпилее изкуствено своето его и се разтвори в колективната душа. Обществото насърчава този феномен, защото това води до нарастване на броя на послушните консуматори, които подхранват системата.

При условие, че мозъкът и сърцето на индивида принадлежат на масата, той не може да има истински морално поведение, защото не знае как да го прави. Масата няма морал, защото няма собствена мисъл, разлики и разум. Посредствеността, която й е присъща, определя поведението на членовете й. При събиране на индивиди и образуване на маса, всички нидивидуални задръжки изчезват, а всички жестоки, брутални и разрушителни инстинкти се събуждат и търсят свободно удовлетворяване. Всеки индивид като част от тълпата се връща няколко стъпала назад в цивилизацията. Самият той може да е бил цивилизован индивид, но „в тълпата се превръща във варварин и придобива спонтанността, необуздаността и свирепостта, присъщи на

първобитните същества, а също и техния ентусиазъм и героизъм“. В тълпата индивидът губи чувството си за отговорност, което играе роля на спирачка за индивидуалните импулси и пориви. Това води до отсъствие на собствени морални ценности и всъщност подтиква към престъпление, насилие и корупция.

Една от характерните особености на съвременния живот е принадлежността на индивида към различни масови движения – политически партии, спортни клубове, религиозни движения, професионални сдружения, синдикати. Това не винаги означава, че в тези групи непременно се наблюдава поведение на психологическа тълпа. За проявата на такова поведение се изискват специални емоционални условия, но никоя организация, дори най - хуманитарната, не е застрахована от този зловещ механизъм. Други по-малки множества са приятелските кръгове и различните клубове.

Поведението на тълпата винаги си остава механично, програмирано, плод на ментално кондициониране, поведение приело формата на подсъзнателно задължение, внушено от пропагандната кампания на властта.

Истинската опасност, която крие масата е нейното отчуждаващо и обезличаващо въздействие върху индивида.

Средностатистическият, „посредственият“ човек е вярно копие на даден модел, чието поведение непрекъснато възпроизвежда. Във вулгарността няма нищо стойностно, а само имитация, пълно отсъствие на креативност, липса на критичност и воля. Обяснение на стремежа на индивида да се „вулганизира“ се намира в обстоятелството, че множеството предлага на субекта редица приятни за неговия животински нагон възможности. Такива са:

- Да се освободи от моралните задръжки, без да изпитва вина.
- Да разтвори своя анемичен и недоразвит „аз“ в големия „аз“ на колективната душа, породена от струпването на много индивиди. Това помага на субекта да забрави собствената си посредственост и да се почувства значим.
- Да се освободи от отговорност изцяло, като убие своя „аз“ и се разтвори в анонимната маса, като при това психологическо самоубийство моралните правила изчезват и човек престава да се чувства подвластен на обществената санкция.

Този анализ позволява да се обясни ситуацията с младежките банди, особено в развитите страни. Членовете на бандата придобиват чувството, че каквото и да направят в нея, колкото опасно и лошо да е то, за тях то престава да бъде такова. Членовете на бандата придобиват чувството, че могат да правят каквото си поискат и че моралните норми не важат за тях.

Днес телевизионният екран и компютърният монитор са най-добрите хипнотизатори.

По ирония на съдбата в съвременния свят всичко е замислено така, че да превърне хората в маса, т.е. да ги „деморализира“, да им отнеме морала, като ги слее с множеството. Деморализацията води непосредствено към заличаване на чувството за съществуване и морал.

Нивото на интелигентност на личността е без значение, тъй като самият факт, че тя е част от определено психологическо множество, елиминира нейния висш разум. То й се възстановява едва след като напусне групата. Това отчасти обяснява безкрайната човешка глупост и ни помага да разберем причините за невероятните грешки, допускани при вземане на важни решения от хора, принадлежащи към психологическо множество.

Генезисът на съдбовни политически или стратегически грешки е именно в тълпата. Поради голямата власт, която получава от обществото, държавникът винаги трябва да е независим и необвързан с никоя политическа партия или психологическо множество, които могат да попречат на висшия му разум. Така би трябвало да бъде поне докато не се открие „ваксина“ срещу отрицателните ефекти, които разглеждаме тук.

Изследвайки психологическата тълпа все повече се убеждаваме, че това е разрушително за разума явление – откровен враг на индивидуалното съзнание.

Оказва се, че неминуемо трябва да се развие някаква дисциплина, която да спаси пълната свобода на индивида, защото неговата инициативност, свобода и талант гинат от най-страшната диктатура – тоталитаризма на масите. Този натиск застрашава непосредствено етиката и висшите ценности на духа, защото истинският морал е съзнателен, а не механичен, но не трябва да се забравя, че съзнателен може да бъде само индивидът, а не масата.

Съвременният човек живее в летаргия, приспан от сливането с човешкото множество, лишен от индивидуален „аз“, направляван от груповия „аз“ или колективната душа. С малки изключения неговият морал не може да бъде по-висок от моралното поведение на множеството.

Оказва се, че ние сме „цивилизовани диваци“, безгрижно лутащи се в живота деца, които си играят с космически станции и ядрени бойни глави.

Измамното усещане за могъщество, което произтича от науката и технологиите, отслабва и притъпява самокритичността на индивида и му пречи да види огромното противоречие между общоприетата версия за цивилизованото човечество и жестоката действителност.

Отчуждението е лишило човека от необходимата воля и ясна мисъл, за да постъпва съзнателно. Летаргичното състояние също не му позволява да осмисли действителния обхват на отчуждението.

Според Джон Бейнс „Това е процес на нашествие, при който в мозъка на индивида прониква чужда или външна информация, завладява неговите неврони, като остава автономна и неподчинена на аза. От този момент тя придобива власт над поведението на индивида, без той да може да се противопостави на въздействието ѝ“.

Причината се крие в погрешните форми на обучение, при които „азът“ отсъства от съзнанието, а мозъкът обработва информацията пасивно. По този начин индивидът се изпълва с „информационен боклук“, със сублиминална информация, която се наслагва в подсъзнанието като безсмислен материал, който отслабва съзнателния „аз“ и води до дезориентация, до емоционални и психологически конфликти. Обикновеният човек се явява „слуга“ - послушен изпълнител на мощните информационни команди, които действат в мозъка му, в резултат на което индивидът е отчужден на самия себе си, без собствени желания и идеали, защото е възприел тези на информационното ядро, което се е превърнало във владетел на невроните и господар на ума му. Доказано е, че колкото повече информация поглъща човек, толкова по-зависим става и толкова по-невъзможно е да се придържа към някакво висше етично поведение. Всяка дейност, всяко обучение – работа, обществен живот, спорт или развлечения се превръщат в елементи, които могат да засилят процеса на отчуждение. Един от най-сериозните проблеми, пред които днес е изправен човешкият ум, е „информационното задръстване“, дължащо се на пресищане на невронните пътища, лавинообразно нарастване на научната и културната инфор-

мация, постоянна сензорна и аудиовизуална атака и крещящия, сензационен и безцеремонен стил на рекламните послания. Всичко това пренасища пътищата на постъпване на информация и блокира висшите мозъчни центрове.

„Светът не притежава истинска етика, нито може да има нравствено поведение, защото нормалното поведение на хората е механично, принудително и програмирано, а програмата не включва солидни, последователни и действителни етични норми“.

Духовният упадък на човечеството е прогресивен, но на пръв поглед това не личи, тъй като е добре прикрит с погрешни и произволни параметри, използвани за измерване на индивидуалния ум. Те не правят разлика между механична пъргавина на мозъка и висша интелигентност, между сляпо подражание и креативност.

Сериозен повод за тревога са незащитеността на мозъка от грубото нахлуване в най-интимните кътчета от съзнанието на индивида, както и функционалната вреда, която нанася на неговите висши способности информационното насищане и блокиране – увреждания на висшия разум, нарушения в способността за съсредоточаване на вниманието, преки поражения върху моралното поведение поради отслабване на характера и волята вследствие на хипертрофия на подсъзнанието и намаляване на съзнателното поведение.

Няма съмнение, че светът страда от потребителско отчуждение „колкото по-голяма е световната витрина на предлаганото за потребление, толкова по-неспокоен и депресиран е човекът“.

Отчуждението е като психическа пандемия, която в определен момент поразява всички хора. Култът към парите, социалният кариеризъм, политиканството, влечението към лукса, хазартните игри, употребата на наркотици, агресивността и насилието, тероризмът, жаждата за власт, завистта, злопаметността, нарцисизмът, сексът като стока за потребление, порнографията са форми на отчуждение, които видимо са завладели големи човешки маси, ръководени от чужд разум и чужди сили, независещи от волята.

Диктатурата на мнозинството лишава индивида от самостоятелност и той е оценяван в зависимост от степента, в която е успял да бъде приет в обществото. В резултат на факта, че на масата са присъщи посредственост и липса на етика, индивидът е осъден на самоунищожение или социална мимикрия.

Съвременното общество се нуждае от сигурност, дефинирана като субективно състояние на човека, при което той се усеща и възприема като уверен, спокоен, живеещ в условия, които не застрашават физическото и психическото му равновесие.

Ето защо въпросът за сигурността на индивида (едно от петте нива на сигурността) е особено актуален в началото на XXI век и неговото решаване е особено важно, още повече, че има отношение и към сигурността на групата и на обществото като цяло.

ЛИТЕРАТУРА

1. Baines, J., (2012) Moral for the 21st Century
2. Boneva, M., (2008), Social ecology, V.T., Faber.
3. Slatinsky, N., (2000), Dimensions of security., S.

ПРЕДАВАНЕ НА ТАЙНИ СЪОБЩЕНИЯ ЧРЕЗ СТЕГАНОГРАФСКИ СПОСОБИ ВЪВ FACEBOOK И GOOGLE+

Светлин Пл. Илиев, Николай Й. Досев, Христо А. Христов

Шуменски университет „Епископ Константин Преславски“ Факултет по технически науки, гр. Шумен

TRANSMISSION OF SECRETS MESSAGES THROUGH STEGANOGRAPHIC METHODS IN FACEBOOK AND GOOGLE +

Svetlin Pl. Iliev, Nikolai I. Dosev, Hristo A. Hristov

Shumen University "Bishop Konstantin Preslavski"

***ABSTRACT**: Steganography (a rough Greek translation of the term Steganography is secret writing) has been used in various forms for 2500 years. It has found use in variously in military, diplomatic, personal and intellectual property applications. Briefly stated, steganography is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. This paper will discuss the possibilities of using steganography via OSN.*

***KEY WORDS**: steganography; OSN; message; transmission.*

Престъпниците от ново поколение, които интегрират технологиите в своите криминални дейности, могат да използват възможностите, които предоставят социалните мрежи, по същите начини, които използват частните или юридически лица. Стеганографията в социалните мрежи, дава възможност за тайно комуникиране, предаване на файлове, легално съхранение на информация в тях и др.

Думата "стеганография" произлиза от гръцката дума "steganos" (скрит, покрит) и "-graph" (рисунка или писание), от които се получава и нейното значение на нещо написано и скрито. Стеганографията се различава от криптографията. При криптографията се вижда текст, който е неразбираем, ако липсва подходящ код за неговото разчитане. В стеганографията, изобщо няма да се разбере, че такъв текст съществува, ако това не се знае предварително, например, ако текстът е написан със симпатично мастило. Например, човек работещ във фирма, занимаваща се с разработка на скъпоструващи лекарства, има достъп до последната разработка на компанията. В същото време, този човек е част от екипа за разузнаване на конкурентна фирма, логично пред него ще възникне въпроса, как да открадне и предаде формулата, по безопасен за него начин. Стеганографията би била един логичен избор, с оглед мерките за сигурност, които подържат в подобни предприятия.[5]

Стеганографският механизъм се състои от „контейнер“, тайно съобщение, прикрепящ алгоритъм, извличащ алгоритъм, стего-ключ и комуникационен канал. По време на стеганограския процес, тайното съобщение се прикрепя към контейнера, с помощта на прикрепящия алгоритъм и стего-ключът, за да се създаде стего-обекетът. Така полученият стего-обект можем да транспортираме, чрез социална

мрежа, e-mail, website, блог, MMS съобщение и т.н. Получателят на стего-обекта, респективно на тайното съобщение, извлича съобщението, чрез извличащият алгоритъм и стего-ключът.[2]

Стегосистемата трябва да бъде направена така, че да ограничи възможностите на "противника" за евентуално разкриване на скритата информация. В качество на данни може да се използва всякаква информация: текст, съобщение, изображение и др., като различните видове стегосистеми скриват тези данни в различни видове "носещи" файлови формати.[1]

"Социална мрежа" е сдружение на хора, съставено заедно със семейство, работа или хоби. Тя е социална структура, съставена от индивиди (или организации), наречени "Възли", които са обвързани (свързани) с един или повече специфични видове взаимозависимост.

Когато комуникацията се извършва, чрез Интернет, тогава говорим за Online Social Network (OSN). Съществуват много определения за социална мрежа, но разработката разглежда социалната мрежа като:" социални мрежи сайтове като уеб-базирана услуга, която позволява на хората изграждане на публичен или полупубличен профил в рамките на ограничена система, артикулира списък на други потребители, с които те споделят една връзка, едно виждане в списъка си на връзки и тези, направени от другите в рамките на система ".[2]

В OSN основното представяне на участниците, е чрез профили. Тези профили могат да съдържат информация, като снимки, възраст, местожителство, месторабота, интереси, приятели, семейно положение и др. Чрез тези профили, участниците комуникират помежду си чрез съобщение, статуси, публикации, снимки, видео и др. В разработката се изследват възможностите за споделяне на снимки във Facebook и Google+. Защото всяка от двете мрежи има своя собствена политика при споделянето на снимки.

Начините за споделяне на снимки във Facebook са три, към тях трябва да се прибави и ключовата опция за споделяне на файлове, с която общо възможностите ни, нарастват до четири. Най-често споделяне се извършва, чрез качване на снимки през функцията „Add Fhotos/Video" или чрез създаване на „Album". И двете функции са достъпни от стените, както на лични профили, така и на стените в групи. Друг начин за изпращане на „контейнер" е чрез опцията за изпращане на снимки, чрез съобщения.

Трите предложени начина подлежат на активна атака, чрез компресия, преоразмеряване, промяна на формата и т.н. Единствения способ, който не подлежи на такива атаки е способа за изпращане на файлове в група. Тези файлове не подлежат на никаква модификация от Facebook. Съществуват три варианта за достъпност до групите, като нивото му, се определя от създателя на групата, при нейното създаване. Трите варианта са – отворена, затворена, и тайна група. Ако една група е отворена, то публикациите в нея и нейните членове ще бъдат видими за всекиго, както и всеки ще може да се включи в тази група. При затворените групи всеки може да види, че съществува такава група, както и нейните членове, но само членовете могат да виждат публикациите в нея. Не така стоят нещата при тайните групи, при тях само членовете на групата могат да видят, че такава група съществува, както и нейните членове и самото й съдържание.

Споделянето на снимки в Google+, е сравнително по-просто от това във Facebook. В Google+ има базова опция за споделяне на снимки „add photo" (добави

снимка), но също така има и опцията “+Share“ функция. Потребителите могат да качат снимка моментално в определения от тях „кръг“ или избран албум. Нововъведение е възможността за изпращане на снимки, чрез съобщения. След проведени експерименти се установи, че тук става въпрос за един и същи обработващ алгоритъм, и в тази връзка ще се разгледат всички тези функции като една. За разлика от Facebook, Google+ не подлага на предварителна компресия качваните снимки. Ако снимката е в съгласие с политиката за качване, то тя ще бъде публикувана без допълнителна намеса. Потребителите могат да ограничат достъпа до снимките си или да ги направят видими за всички, или пък само за определени кръгове. „Кръг“ в Google+ е подобен на списък с приятели във Facebook, като потребител може да създава неограничен брой кръгове, в зависимост от нуждите си. Кръговете могат да се обособят като приятелски, познати, семейство и т.н.[2]

Предимството, при използването на Google+ за транспортирането на стеганографски изображения, генерирани от JP Hide and Seek, S-Tools, StegHide, HIP, GIF-it-Up, F5, SteganPEG, SilentEye и т.н. ще бъдат качени директно, стига те да са във формат JPEG, BMP, PNG или GIF, и да не надвишават 2048 пиксела в широчина или височина. Снимките, ще бъдат транспортирани, без никаква намеса от страна на платформата. Важно е да се отбележи, че „контейнери“ създадени, чрез SilentEye са видимо изменени, което непременно ще събуди подозрителност на даден етап, за това се препоръчва използването на различен софтуер. Също така е препоръчително използването на „контейнери“ във формат JPEG, защото той е най-използваният формат в Интернет. [4]

В таблица 1, могат да се видят данните, които се отнасят за Facebook и са събрани по време на експеримента. Както се вижда от четирите функции за споделяне на снимки, само функцията, чрез прикрепяне дава 100% успех. Вижда се промяната в имената на сваленитe файлове, а също така и променениият размер. Например снимка, изпратена чрез съобщение и озаглавена Stego JPEG – S, при изтеглянето ѝ тя вече е озаглавена - 10416773_1407170579570141_1125128837_n. Тя също така е променила размера си от 2 244 662 bytes на 116 151 bytes. MD5 стойностите ѝ, също са различи - 59C36687A164D0BC7CDB2A6BA84E974 при качване и 59C36687A164D0BC7CDB2A6BA84E9743 при сваляне. Както се предполага, извличането на съобщението бе невъзможно.

Таблица 1. Стойности и данни за способ, оригинално заглавие, успех за извличане, първоначален размери, размер при сваляне и изходен формат

№	Способ	Име на файла при качване	Успех извличане на информация	Размер със стего файла	Размер при сваляне	Изходен формат
1	Качване на снимка	Stego BMP - MBPS	НЕ	406 998 bytes	17 411 bytes	JPEG
2	Чрез съобщение	Stego BMP - MBPS	НЕ	406 998 bytes	17 411 bytes	JPEG
3	В група	Stego BMP - MBPS	НЕ	406 998 bytes	17 411 bytes	JPEG
4	Прикрепяне	Stego BMP - MBPS	ДА	406 998 bytes	406 998 bytes	BMP
5	Качване на снимка	Stego BMP - S	НЕ	406 998 bytes	17 417 bytes	JPEG
6	Чрез съобщение	Stego BMP – S	НЕ	406 998 bytes	17 417 bytes	JPEG

7	В група	Stego BMP – S	НЕ	406 998 bytes	17 417 bytes	JPEG
8	Прикрепяне	Stego BMP – S	ДА	406 998 bytes	406 998 bytes	BMP
9	Качване на снимка	Stego BMP – SE	НЕ	406 998 bytes	17 417 bytes	JPEG
10	Чрез съобщение	Stego BMP – SE	НЕ	406 998 bytes	17 417 bytes	JPEG
11	В група	Stego BMP – SE	НЕ	406 998 bytes	17 417 bytes	JPEG
12	Прикрепяне	Stego BMP – SE	ДА	406 998 bytes	406 998 bytes	BMP
13	Качване на снимка	Stego JPEG - BMPS	НЕ	2 244 662 bytes	92 672 bytes	JPEG
14	Чрез съобщение	Stego JPEG - BMPS	НЕ	2 244 662 bytes	116 153 bytes	JPEG
15	В група	Stego JPEG - BMPS	НЕ	2 244 662 bytes	92 672 bytes	JPEG
16	Прикрепяне	Stego JPEG - BMPS	ДА	2 244 662 bytes	2 244 662 bytes	BMP
17	Качване на снимка	Stego JPEG – S	НЕ	2 244 662 bytes	92 687 bytes	JPEG
18	Чрез съобщение	Stego JPEG – S	НЕ	2 244 662 bytes	116 151 bytes	JPEG
19	В група	Stego JPEG – S	НЕ	2 244 662 bytes	92 687 bytes	JPEG
20	Прикрепяне	Stego JPEG – S	ДА	2 244 662 bytes	2 244 662 bytes	JPEG
21	Качване на снимка	Stego JPEG - SE	НЕ	38 541 bytes	45 477 bytes	JPEG
22	Чрез съобщение	Stego JPEG - SE	НЕ	38 541 bytes	72 171 bytes	JPEG
23	В група	Stego JPEG - SE	НЕ	38 541 bytes	45 477 bytes	JPEG
24	Прикрепяне	Stego JPEG - SE	ДА	38 541 bytes	38 541 bytes	BMP

Google+ е изключително приветлива платформа, що се отнася до стеганографията. Всички софтуерни програми, които бяха използвани при експеримента, успяха да предадат тайното съобщение. Освен това, Google+ приема много от най-често срещаните формати, като JPEG, PNG,BMP и GIF, без да ги изменя. Това се потвърждава от непроменените MD5 стойности на изображенията. Платформата позволява разделянето приятели на общности или по-точно „кръгове“. В таблица 2, са дадени получените резултати, които се отнасят за Google+.

Таблица 2. Стойности и данни за софтуерен продукт, MD5 стойности, формат, успех

№	Програма	Име на файла при качване	HASH	Успех	Изходен формат
1	BmpSecrets	Stego BMP - MBPS	B1F5E28BEC7B648D6840FAF76495C1AA	ДА	BMP
2	Steganographystudio	Stego BMP - S	16E58AAAEB78169A55E72DDFCAE95CC8	ДА	BMP
3	SilentEye	Stego BMP - SE	82835494441D89B4DC9D7FFBC1062610	ДА	BMP
4	BmpSecrets	Stego JPEG - BMPS	83E55856F7872C042599648F19DC71B3	ДА	JPEG
5	Steganographystudio	Stego JPEG - S	781BDE4FECD5A0A8EB84EAADC0CF33D6	ДА	JPEG
6	SilentEye	Stego JPEG - SE	11A2A80900A38C456DB0365E5EB4E28D	ДА	JPEG

Повечето от софтуерните продукти, достъпни в Интернет, не биха могли да пробият активната атака от страна на Facebook при споделянето на снимки. Всички софтуерни продукти работещи с формати различни от JPEG, вещаят висок процент на неуспеваемост при предаване на съобщението. Това се дължи главно на факта, че Facebook преобразува всички други формат в JPEG. Стеганографията все пак е възможна, чрез опцията за прикрепяне на файлове в група.

Поддържането на много видове формати и 100% успеваемост при извличане на информацията, правят Google+ атрактивна платформа, що се отнася до стеганография. Възможността и за споделяне, чрез само две функции (споделяне и чрез съобщение), я правят по-лесна за работа и не привличаща толкова внимание. Авторите ще предложат, да не се използва SilentEye. Въпреки че, продуктът предава съобщението чрез платформата, изображението драстично променя качеството си и може да предизвика ненужно внимание.

Експериментите показаха, че Facebook има повече функции за споделяне, но пък от своя страна Google+ е достъпна за повече техники. Ограничеността от страна на поддържани формати, правят Facebook доста ограничен откъм възможности за предаване на тайни съобщения. Освен това, цели три от четири възможни функции за споделяне, провеждат активна атака върху споделените изображения, чрез промяна в размера, името и формата им. Възможността за успешно предаване, само чрез четвъртата функция(прикрепяне на файлове), може да предизвика ненужно внимание. Споделянето в Google+ със своите две функции за споделяне, от които функцията за споделяне на снимки е главна, не е толкова „набиващо се на очи“.

Беше установено, че програмата за прикрепяне на тайни съобщения SilentEye, променя очевидно първоначалният вид на изображението.

Изследването доказа, че е възможно използването на стеганография в социалните мрежи. Това твърдение обаче, има някои ограничения относно Facebook. Стеганография, чрез прикрепянето на данни към „контейнер“ и споделянето му във Facebook или Google+, е напълно възможно и реално. Проблема, които се появява при Facebook е извличането на скритото съобщение, в следствие обработка на снимката, но все пак има възможност за използването на платформата. Новата опция за споделяне на файлове във Facebook, е тайната вратичка, която би могла да се използва за предаване на „контейнери“. Файловете могат да бъдат от всякакъв формат, стига той да не е .mp3 или .exe и да влизат в ограничението за размер – 25 MB. В експеримента, беше доказано, че SteganographyStudioи BPMSecrets, могат да предадат „контейнер“ със стеганографска информация, а SilentEye позволи извличането на тайното съобщение, но трябва да се отбележи, че снимката променя коренно своето качество. Толкова явна манипулация на снимка, непременно би породила съмнение.

Експеримента се проведе върху двете най-големи социални мрежи в момента – Facebook и Google+. И двете мрежи имат по три функции за споделяне на снимки – качване на снимка, прикрепяне към съобщение и споделяне. Facebook от своя страна има и четвърта опция за споделяне на файлове. Снимките споделени по този начин не претърпяват никаква модификация и извличането на съобщението е с успеваемост 100%. Извличането на информация от „контейнер“ от Facebook се препоръчва единствено, чрез опцията за споделяне на файлове. Останалите функции за споделяне се оказаха ненадеждни. Това се дължи на преоразмеряването, което прави мрежата с всяка качена или изпратена снимка. Също така, при разли-

чен формат освен .jpg, той веднага бива променян. Google+ е много по-подходящ при изпращането на „контейнери“ през социалните мрежи, поради своята политика по отношение на споделяните и изпращаните снимки.

Експериментът доказа, че рутинността, която са добили социалните мрежи в своето използване, се явява проблем, пред защитата от използване на стеганографски способи. Един от основните белези, е че използването на социалните мрежи за споделяне на снимки и друг вид файлове, е нещо съвсем нормално в днешно време и не буди подозрения. Още един факт, който подкрепя нуждата от изследване на възможностите за стеганография в социалните мрежи е, че тези методи могат да бъдат използвани от хора без специализирано техническо образование.

В заключение може да се каже, че опасността от тайно комуникиране в социалните мрежи е напълно реална. В перспектива ще се направи по-задълбочено изследване на комбинациите между различните типове стеганография.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Marvel, L. M., Jr, C. G. B. & Retter, C. T. (1998) Reliable Blind Information Hiding for Images. *Second International Workshop on InformationHiding, IH'98,* 1525**,** 48-61.

2. Lee, Y. K. & Chen, L.-H. (2000) High Capacity Image Steganographic Model. IEE Proceedings of Vision, Image and Signal Processing, 147, 288-294.

3. Iso-Dis (1992) Digital Compression and Coding of Continuous-Tone Still Images - Requirements and Guidelines. CCITT Recommendation T.81.

4. Crouse, M. & Ramchandran, K. (1995) Joint Thresholding and Quantizer Selection for Decoder-Compatible Baseline JPEG. International Conference on Acoustics, Speech, and Signal Processing. ICASSP-95, 4, 2331-2334.

5. Станев, С. Стеганологична защита на информацията. Университетско издателство, Шумен-2013, ISBN 978-954-577-825-4.

ЕВОЛЮЦИЯ В СХВАЩАНИЯТА ЗА СИГУРНОСТТА

Калин И. Кръстев

Университет по библиотекознание и информационни технологии , гр. София

Христо А. Христов

Шуменски университет „Епископ Константин Преславски”

EVOLUTION IN PERCEPTIONS FOR THE SECURITY

Kalin I. Krastev

University of library studies and information technologies, Sofia

Hristo A. Hristov

Shumen University “Bishop Konstantin Preslavski”

***ABSTRACT**: National security and defense are fundamental to the existence and stability of any country. Development of public ideas for ensuring national security demands the more accurate specification of this concept.Unfortunately, practice and theory do not provide an established definition. National security is poorly defined concept.Definition problem really exists,which leads to either close guidance of policies and activities to ensure the security.*

***KEY WORDS**: national security,security, defense paradigm, democracy and democratic principles, threats and risks.*

“Сигурността е като кислорода - не я забелязваш, докато не започнеш да я губиш. Ала тогава вече ти не можеш да мислиш за нищо друго на света, освен за нея”. [1]

Сигурността не е самостоятелна наука, дори, строго погледнато, не съществува единна теория на сигурността, така че нейният предмет не може да се определи еднозначно. [2]

Според други спектърът на сигурността трябва да бъде спестяван, за да се заделят достатъчно ресурси за осъществяване на реална политика на сигурност.

Според Пламен Пантев терминът „сигурност” *„...отразява основна категория на изследванията и на практиката на международните и вътрешнополитическите отношения*”. [3]

Според Георги Стефанов „*Предметът на Теорията на международната сигурност не е сигурността на една или друга държава, не е състоянието на сигурността в отделен регион, на глобалните отношения или конкретните аспекти на*

сигурността на един или друг практически външнополитически интерес. Предмет на изследване е самата сигурност като същност, като феномен. Предмет са елементите на нейния абстрктен модел, начините и средствата за нейното поддържане и защита, формите и равнищата ѝ, както и взаимодействията между тях". [4]

Според някои изследователи област на сигурността може да бъде „всеки аспект на международните и вътрешнонационалните отношения".

Николай Слатински смята, че: „*С развитието на демокрацията Сигурността изживява дълбока и многопосочна еволюция. Тя завинаги е свалена от пиедестала на абсолютната денност. Демокрацията снема ореола ѝ на абсолютно благо и я прави относително благо, което не само предпоставя нагласите, стремленията и целите на хората, но се превръща и в тяхна функция*". [5]

Понятието „*сигурност*" е тясно свързано с категорията „*национални интереси*". Нещо повече, първото е производно от второто. Националната сигурност е призвана преди всичко да гарантира ненакърнимостта на основните, жизнено важни интереси: националният суверенитет, териториалната цялост на държавата и защитата на нейното население – т.е. такива интереси, за постигането на които поскоро се воюва, отколкото се върви към компромис. Иначе казано, националната сигурност – това е стратегия, насочена към осигуряване на жизнено важните интереси на националната държава. Това е класическият, реалистки подход към проблема. [6].

За първи път понятието "Национална сигурност" е употребил президентът на САЩ Теодор Рузвелт в обръщение към Конгреса през 1904г., обосновавайки присъединяването на зоната на Панамския канал с интересите на националната сигурност [7]. А първото определение на националната сигурност в категориите на "националните интереси" е дадено от Уолтър Липман: "Държавата се намира в състояние на сигурност, когато не ù се налага да принася в жертва своите законни интереси, за да избегне войната и когато тя е в състояние да защити при необходимост своите интереси чрез водене война".[8]

Речникът на военните термини на Министерството на отбраната на САЩ, издаден от Комитета на началник-щабовете, придава на националната сигурност ярък проамерикански дух и американоцентричност, определяйки я като "Сфера на прилагане на съвместните усилия на военната и външната политика на страната и като желано условие за нейното развитие, обезпечавано преди всичко чрез американско военно и отбранително превъзходство над всяка чуждестранна държава или група държави, чрез благоприятна позиция в международните отношения, а също чрез способност за отбрана. Съвкупността на тези фактори позволява успешно да се противостои на враждебни или разрушителни, явни или скрити действия на други страни, включително на прилагане от тях на военна сила."[9]

В Закона на Руската Федерация "За сигурността", националната сигурност е "състояние на защитеност на жизнено важните интереси на личността, обществото и държавата от вътрешни и външни заплахи."[10]

В Руския Енциклопедически речник "Политология", националната сигурност е дефинирана като: "Състояние, при което се обезпечава защитата на жизнено важните интереси на държавата и гражданското общество в икономическата, политическата, военната, екологическата, хуманитарната и други области".[11]

В Концепцията за национална сигурност, приета от кабинета на Жан Виденов през 1995г. и негласувана от парламента, е дадено определението: “Националната сигурност е динамично състояние, при което за държавата и обществото не съществува пряка опасност от въоръжена агресия, политически диктат или икономическа принуда, или ако такава се появи, те ще бъдат надеждно защитени.”[12] По-рано, в приетата от същото правителство и неодобрена от Народното събрание Военна доктрина се посочва, че: ”Националната сигурност се счита за гарантирана, когато държавното ръководство прецени, че не съществува заплаха за националните интереси или заплаха от всякаква форма на насилие и принуда, или, че тази заплаха може да бъде компенсирана, неутрализирана или управлявана.”[13]

Според официално приетата през 1998 г. Концепция за национална сигурност: “Национална сигурност има, когато са защитени основните права и свободи на българските граждани, държавните граници, териториалната цялост и независимостта на страната, когато не съществува опасност от въоръжено нападение, насилствена промяна на конституционния ред, политически диктат или икономическа принуда за държавата и е гарантирано демократичното функциониране на държавните и гражданските институции, в резултат на което обществото и нацията запазват и увеличават своето благосъстояние и се развиват. Сигурността е гарантирана, когато страната успешно реализира националните интереси, цели и приоритети, и при необходимост е в състояние ефективно да ги защити от външна и вътрешна заплаха."[14]

През 1999г., Н. Слатински предлага „Схема на петте нива на сигурността” [15].

Първото ниво е **сигурност на индивида** (на личността, на отделния човек) - наричана различно: лична, индивидуална, персонална сигурност; съответно human/individual/personal security. Тя излиза все повече на преден план, защото е свързана пряко не просто с правото на живот, а с правото на по-добро качество на живот, с другите основни човешки права и задължения, свободи и отговорности.

Второто ниво е **сигурност на групата** (от хора) - групова сигурност, group security. Групата може да се обособи по различни признаци: етнически, религиозен, социален, професионален, сексуален. Напр., такива групи са малцинствата. Тук се включват различни обществени прослойки, като краен вариант - самото общество. Групата носи в себе си материални и духовни ценности, идентичност, памет, език, традиции, обичаи. Опазването и зачитането им е важен аспект на сигурността ù.

Третото ниво е **сигурност на държавата** - държавна сигурност state security. Тя е свързана със защитата на изконни ценности: териториална цялост, независимост, суверенитет, конституционен ред и др.

Четвъртото ниво е **сигурност на общността** (от държави) - т.е. колективна, коалиционна сигурност, или collective/community/alliance/coalition security. Терминът "общност" обхваща различни форми на сдружаване на държави: двустранни и многостранни договори и пактове, общности за сигурност, коалиции, съюзи и др.

Петото ниво е **сигурност на света** (на планетата) - т.е. глобална, универсална, обща, всеобща сигурност, съответно global/common/cooperative security. При нарастващата взаимообвързаност, проблемите на глобалната сигурност постепенно излизат на преден план. Ръководената от Улоф Палме Независима комисия по въпросите на разоръжаването и сигурността към ООН първа разработи в началото на 80-те години концепцията за обща сигурност(common security), съгласно която не може да има трайна сигурност, ако тя не бъде споделена от всички и че обща си-

гурност може да бъде постигната само чрез сътрудничество, основано на принципите на равенството, справедливостта и реципрочността.[16]

Първите три нива на сигурността - на човека, на групата, на държавата определят **националната сигурност.** [17]

Сигурността на държавата е сечението на националната и международната сигурност. Държавата е основен, но не и единствен актьор на националната сцена, затова няма знак за равенство между държавна и национална сигурност. Схемата отчита важността на сигурността на различните общности от хора за националната сигурност и, не на последно място, тя е в крак със засилващото се човешко измерение на сигурността като ключов елемент на националната сигурност.

Според Георги Стефанов: "Сигурността е най-общ показател за ефективността на външната политика" [18]. А съгласно чл. 24, ал. 2 на нашата Конституция националната сигурност е основна цел на външната политика на страната [19]. Джон Стюарт Мил определя сигурността като интерес от висш порядък, задължаващ към защита на това, което е необходимо за благосъстоянието на гражданите на държавата [20]. За Васил Проданов: "Националната сигурност е основно морално и политическо право на всяка държава, висше благо и цел, една от най-важните категории при вземането на политически решения."[21] А Джон Херц разглежда международните отношения като "**security game**" - игра на (за) сигурност [22].

Сигурността днес се разбира като повече от "без-опасност". Г. Стефанов формулира две нива на сигурност: безопасност и гарантирана надеждност [23]. Илия Пеев сочи някои "измерители на сигурността": липса и отсъствие на опасност, гарантирана безопасност и сигурност, защитеност, застрахованост, неприкосновеност [24].

Според Арнолд Уолфърс, сигурността, подобно на благосъстоянието, е сред основните социални ценности [25]. За Джон Бъртън сигурността е сред базисните индивидуални и групови потребности, и то такива, които се отстояват независимо от цената [26]. Широко известна е йерархията на потребностите на Абрахам Маслоу. Сред тях на второ място е нуждата от "safety" и "security" - преведени като "безопасност" и "сигурност". Тази нужда е непосредствено над физиологичните потребности - глад, жажда, сън, отопление, секс и др., "които веднъж задоволени, повече не влияят върху поведението на човека"[27] и отразяват (ако изобщо отразяват), в крайно слаба степен индивидуалността на личността. Нуждата от сигурност е първата, в която зримо се проектира човешката индивидуалност и поражда у човека стимул за взаимодействие с другите хора и подбуди за себеизява и творчество. Ил. Пеев описва сигурността като доминираща категория за определяне на психическото здраве на човека. "Без да се удовлетвори потребността от сигурност - човекът и човешките маси не могат да удовлетворяват потребностите от висш ранг. Такива висши потребности не могат да бъдат мотиватори в дейността на хората, без да се гарантира тяхната сигурност!"[28]

За всяка жива система е естествен стремежът към повече сигурност. Затова за В. Проданов: "Сигурността е характеристика на всяка система и тя е в нейната способност да се съхрани при промяна на средата, условията и обстоятелствата, от които зависи; да функционира и се развива оптимално, т.е. при най-малък разход на ресурси да осъществява заложените в нея закономерности и цели."[29] А Г. Стефанов сравнява сигурността с температурата на тялото – "първостепенен и генерализиращ показател за състоянието на организма и за наличието или отсъствието на някакво болестно състояние."[30]

Карл Дойч пише за своеобразен закон на Паркинсон за националната сигурност: чувството за несигурност на една нация нараства успоредно с нейната сила/мощ [power] [31]. Колкото повече мерки за да гарантира сигурността си предприема тя, толкова по-несигурна се чувства. Като всеки друг "закон", и този е парадоксална интерпретация на познат факт. Чувството за несигурност зависи както от реалните въздействия, така и от начина по който системата ги възприема и оценява. Арнолд Уолфърс различава субективна и обективна сигурност. Субективната сигурност се свързва с отсъствието на страх от заплаха, обективната сигурност - с отсъствието на заплаха. За да има истинска сигурност и обективната, и субективната сигурност трябва да са налице [32]. Щом сигурността е субективно усещане, колко сигурост е потребна, за да се чувства нацията сигурна? С манипулации, заплахи, внушения може да се понижи рязко усещането за сигурност. Как тогава да се определи кога обществото е настина сигурно? То лесно може да бъде тласнато в грешна посока – да търси повече сигурност, отколкото му е необходима. Или да преглътне всичко с мисълта – да става каквото ще, да правят каквото щат, само мир да е! С други думи – единственото, което запазва своята ценност тогава е мирът. Мирът като съгласие да се живее в по-малко сигурност, само и само да се избегне войната.

Съществуват различни класификации на отделните аспекти на сигурността, т.е. на видовете сигурност.

Първата класификация дава основните компоненти на сигурността. Свързана е със спектъра на рисковете и заплахите към нея. В този случай сигурността бива военна, икономическа, социална, етническа, екологическа, информационна и др.

Втората класификация слага акцента върху способа, по който се "атакува" сигурността – дали чрез материално въздействие, т.е. твърда сигурност (hard security) или чрез нематериално влияние (*soft security*). При твърдата сигурност се работи с измерими величини/потенциали – сила, натиск, армия; това са *sticks* – тоягите, санкциите, наказанията и др.; докато при меката сигурност имаме идеи, манипулация, дезинформация; това са *carrots* – морковите, поощренията, наградите). При първия случай заплахата е по-пряка, по-откровена и по-груба, а при втория – по-индиректна, по-префинена и по-коварна.

Третата класификация се прави според посоката, от която идват заплахите и предизвикателствата към сигурността: дали от фактори, източници, субекти извън националната държава или в нея; тя дели сигурността на външна и вътрешна.

Многозначността на понятието национална сигурност отразява субективизма в схващанията за него. Желателна е обаче някаква обща степен на концептуализиране на понятието, която ориентира политиците и прави възможен общественото съгласие и контрол на техните решения и действия.

Усилията за очертаване на понятийното съдържание не са постоянни. Ясно се забелязват периоди на интензификация на този стремеж. Настоящия период на международни отношения, маркиран с края на студената война, е период на редефиниране на това понятие за нашата, а и за засегнатите от промяната страни. Очевидно вниманието към националната сигурност расте в периоди на криза, в които обществото ясно забелязва незадоволителността на съществуващите концепции, след неуспешно справяне с нововъзникнали заплахи. Подобни примери за страната са периодите на повишено внимание към икономическата сигурност през седемдесетте и екологическата сигурност през осемдесетте години.

Може да се направи извод, че по-общото дефиниране подсказва усещане за по-голяма отвореност и несигурност, и вглеждане в по-широк кръг от потенциални заплахи за страната. Обратно по-тясното тълкуване е следствие на вътрешна затвореност и търсене на гаранции в традиционните силови средства за сигурност.

В страната няма законодателен акт, които да обхване детерминантите на националната сигурност. Най-значещите от тях – външната политика, вътрешната политика, отбраната, икономиката имат или преминават правно нормиране, но не са системно подчинени на общите цели на сигурността. Още по-малко са дефинирани връзките на други сфери на обществената практика със сигурността. Индустрия, селско стопанство, търговия, финанси, наука, образование, здравеопазване, социална защита остават необвързани с проблема сигурност.

Сигурността е антитеза на несигурността. И двете понятия тук се отнасят към състоянието на националната обществена система. Отразяват вероятност за преход на системата от желано, гарантиращо изпълнението на мисията, състояние в нежелано и негарантиращо мисията състояние. По-голямата сигурност означава по-малка вероятност за преход и неизпълнение на мисията.

Сигурността е мярка за комплексната възможност на системата да изпълни целевата мисия. По-абстрактно погледнато тази възможност е функция на способностите да бъде постигната мисията в условията на благоприятна, безразлична или неблагоприятна среда.

Сигурността на националната система е съставена от вътрешната и външна сигурност. Тя е неделима от сигурността на субрегиона, региона и света, поради открития характер на обществените системи и тяхната взаимозависимост.

Пряко свързани с проблема сигурност са въпросите за ролите, рисковете и отговорностите, които трябва да поеме страната за да вгради своето място в общата и неделима система за сигурност. Произтичащи от това са и измеренията на политическата, икономическата и военна сигурност, с които страната ще съгражда общата сигурност.

Класическото схващане за национална сигурност се свежда обикновено до гарантиране на националната цялост, независимост и суверенитет.

Традиционно националната сигурност означава военна сигурност на страната и директно се свързва с нейната отбрана и силова структура. В този тесен аспект на понятието вниманието се насочва към характеристика на потенциалните конфликти, от които се опитва да изведе потребните качества на силовата структура.

В своето функциониране системата за сигурност и отбраната са изправени пред множество рискове, заплахи и предизвикателства. Всички те трябва да бъдат държани под контрол, идентифицирани и оценявани в зависимост от влиянието им за сигурността. През 1983г. Ричард Улман дава интересно определение на заплахата, като приема, че "тя е действие или последствие от събитие, което застрашава силно в момента или в относително кратко време да разруши качеството на живота на жителите на страната или заплашва значимо да стесни гамата от политически алтернативи, разполагаеми от правителството на държавата или от личните неправителствени същества (хора, групи, корпорации) в държавата".

Първият компонент на това определение е логичен тъй като качеството на живота е ценност от най-висок порядък за обществото. Вторият компонент обаче подчертава либералния характер на държавата и нейната главна функция-да защити индивидуалните права и правото си да избере адекватни политически решения.

Заплахата е неотделима от рисковете, пред които тя изправя обществото на националната държава. Рисковете са потенциални загуби, които най-общо могат да се разделят на военни и невоенни. Преките засягат територията и гражданите, а непреките интересите на държавата или нейните съюзници.

Невоенните рискове могат да бъдат политически, икономически, социални, природни, екологически, информационни и т. н. Политическа нестабилност или икономическа кризисност, природни катастрофи, тероризъм, международна престъпност могат да предизвикат вътрешна несигурност, а някои от тях и война. Сложно е комбинирането на различните видове заплахи и трудно предвиждането на тяхната трансформация в действия на потенциален опонент. Още по-трудно е това в случаите с участваща военна заплаха, при която потенциална военна мощ се комбинира с политически намерения и действия за нейното използване срещу нечии интереси. Още по-трудно определима е ситуацията на комбиниране на политическа нестабилност и икономическа кризисност и значителна военна мощ, която може да се превърне в изкушение за незрелите политически сили.

Анализът на понятието "сигурност" не би бил пълен, ако не се спрем на задълбочаващите се нейни различия с две други архиважни понятия - "мир" и "отбрана", с които сигурността доскоро се смяташе за почти идентична.

В Устава на ООН съчетанието "мир и сигурност" се употребява 105 пъти [28]. На практика в този исторически документ мирът и сигурността са синоними. Трудно би могло да бъде другояче, след като светът все още е в развалини след най-унищожителната война в своята история. Днес обаче има ли сигурност, има и мир, но обратното вече не е вярно. Сигурността е много повече от мира. Дори с магическа пръчка да бъдат овладени непрекъснато избухващите конфликти и в един миг да настъпи мир на планетата, все едно - тя още дълго време няма да се радва на сигурност, защото остават активни проблеми, чиито последствия могат да направят дните на човечеството преброени в буквалния смисъл на думата.

Отбрана и сигурност също все повече се отдалечават една от друга по смисъл и съдържание. В управлението и защитата на държавата сигурността е преди всичко приоритет на политиците, а отбраната - на военните (разбира се, самата отбрана вече не е само военен въпрос, тя все повече се превръща в политически проблем). Сър Джеймс Еберле пише: “Политиката за сигурност преследва политически цели; отбранителната политика - военни цели. Сигурността включва процесите на политически диалог. Отбраната включва структурата и действието на въоръжената сила. Сигурността включва рискове и предизвикателства, които са извън полето на военната компетентност. Отбраната в крайна сметка почива върху способността на въоръжените сили да вземат връх по време на война.”[33] Отбранителната недостатъчност днес все по-успешно може да се компенсира с мерки за укрепване на сигурността.

В заключение може да се посочи, че проблемите на сигурността са почти винаги екзистенциални, а решенията им са най-често политически. Тези проблеми, могат да се управляват сравнително успешно и до определен момент, само докато водят до количествени, и много по-трудно, когато водят до качествени промени. Един проблем на обществото става проблем на сигурността, или както се казва в западната литература – секюритизира се, когато като резултат от него могат да възникнат качествени промени, когато обществото не може да го абсорбира без структурни трансформации. Борбата с тероризма и заплахите произтичащи от

същия, като елемент от гарантирането на сигурност трябва да започва на възможно най-ранен етап, да се използват и усвояват разнообразни и ефективни форми и методи за управление, както и гъвкавото им подменяне с оглед резките изменения в обстановката. Очевидно е, че за да се реагира своевременно на широкия спектър и динамичния характер на заплахите, ще трябва да се използват високите възможности на съвременните електронно-информационни средства, както и предварително разработени модели за тяхното управление.

Новите реалности в света и в Европа, натрупаният от страната ни международен авторитет и последователната ú принципна политика на добросъседство и сътрудничество са важна предпоставка за успешното отстояване на националните интереси и сигурност. Съществуващите днес рискове и заплахи за националната сигурност изискват съвършено нов тип подход, образование и обучение на служителите от институциите, ангажирани и отговорни за гарантирането на националната сигурност и мир в страната, адекватни на променената стратегическа среда и новите мисии. Настъпващите промени налагат разработването и актуализирането на концепцията за национална сигурност, военната доктрина и национална военна стратегия на Република България. Те ще наложат промени в отделните доктрини за използването на войските и силите на оперативно и тактическо ниво.

ЛИТЕРАТУРА:

1. Джоузеф Най-младши, Уилям Оуънс, “Информационното острие на Съединените щати”, “Военен журнал”, No. 3, 1996, стр. 56.

2. Д. Кръстев „Политика на ЕС в областта на сигурността”, „Военно издателство” ЕООД, 2010г., стр. 11

3. Пл. Пантев, „Международните преговори в областта на сигурността”. Сиела, 2006г., стр. 35

4. Г. Стефанов, „Теория на Международната сигурност”. Сиела., 2005, стр. 9

5. Н. Слатински, „Националната сигурност: аспекти, анализи, алтернативи”., Сиела., 2004г., стр. 121

6. Д. Кръстев „Политика на ЕС в областта на сигурността”, „Военно издателство” ЕООД, 2010г., стр. 12

7. АН СССР, Авторский коллектив, "Современные буржуазные теории международных отношений (критический анализ)", М., “Наука", 1976, здесь стр. 332.

8. Владимир Петровский, "Доктрина "Национальной безопасности" в глобальной стратегии США", М., "Международные отношения", 1980, стр. 323.

9. И. Жинкина, О понятии “безопасность государства”, “США-ЭПИ”, No. 9, 1995 г., стр. 58.

10. Камалудин Гаджиев, "Геополитика", стр. 374.

11. Ю.И.Аверьянов, "Политология”, стр. 197.

12. Концепция за национална сигурност на Република България, “Международни отношения”, №. 3, 1995 г., стр. 98.

13. Военна доктрина на Република България, “Военен журнал”, No. 3-4, 1994, раздел 8.

14. Концепция за националната сигурност на Република България, "Държавен вестник", брой 46, 22.04.1998 г., стр. 1-5.

15. The Commission on Global Governance, "Our Global Neighbourhood", Report, 1994, www version.

16. Н. Слатински “Измерения на сигурността” София, Издателство “Парадигма”, 2000г., стр. 20-21

17. Георги Стефанов, "Международната сигурност", С., "Сиела", 1997 г., стр. 9.

18. Конституция на Република България, "Държавен вестник", бр. 56, 13.07.1991 г.

19. Татьяна Алексеева, "Дилемма безопасности: американский вариант", "Полис", No. 6, 1993 г., стр. 19.

20. Васил Проданов, “Вътрешната сигурност и националната държава”, “Военен журнал”, No. 2, 1995, стр. 9.

21. John Herz, "International politics in the Atomic Age", New York, Columbia University press, 1962, p. 3.

22. Георги Стефанов, "Международната сигурност", стр. 11-16.

23. Илия Пеев, “Психологически аспекти на сигурността”, стр. 33-46, във: “Сигурност чрез партньорство и интеграция. България, НАТО и европейската архитектура на сигурност”, БЕКСА, София, 1996, стр. 37.

24. Jef Huysmans, "Security! What Do You Mean? From Concept to Thick Signifier", "European Journal of International Relations", Vol. 4, No. 2, June 1998, page 233.

25. John W. Burton, "Conflict Provention as a Political System", pp. 115-127, in: John A. Vasquez, James Turner Johnson, Sanford Jaffe, Linda Stamato (edts.), "Beyond Confrontation. Learning Conflict Resolution in the Post-Cold War Era", Ann Arbor, The University of Michigan Press, 1995, page 120.

26. Райна Стойнешка, Илия Пеев, "Икономическа психология", Варна, "ТедИна", стр. 55.

27. Илия Пеев, “Психологически аспекти на сигурността”, стр. 38-39.

28. Васил Проданов, “Вътрешната сигурност …”, стр. 8.

29. Георги Стефанов, "Международната сигурност", стр. 9.

30. Karl Deutsch, "The Analysis of International Relations", New Jersey, Prentice-Hall, Inc., 1968, page 88.

31. Barry Buzan, Ole Wæver, Jaap de Wilde, "Security. A new Framework for Analysis", Lynne Rienner Publishers, Boulder London, page 30.

32. Георги Стефанов, "Международната сигурност", стр. 9.

33. Сър Джеймс Еберле, "Интересите на Западна Европа в областта на сигурността", стр. 139-151, във: “Информационен политически сборник", БАН, ИПИ, брой 1, С., 1991 г., стр. 143.

ПРОБЛЕМЪТ ЗА ДОМАШНОТО НАСИЛИЕ

Красимир М. Марков

Шуменски университет „Епископ Константин Преславски”
Педагогически факултет

PROBLEM OF DOMESTIC VIOLENCE

Krasimir M. Markov

ABSTRACT: *Discusses the problem of domestic violence. With the main attention to violence against women and its psychological implications.*

KEY WORDS: *domestic violence victims, psychology*

Проблемът за насилието е един от най-наболелите проблеми разработвани от психолозите в света. Най-общо насилието се определя като принудително въздействие от някого върху някого. Съществуват много класификации на насилието, но се е наложила тази, която го определя в зависимост от характера на насилствените действия. Автори като Алексеева (2000) приемат, че то може да бъде класифицирано на физическо, сексуално, психологическо (емоционално) и икономическо [1]. Тя разглежда физическото насилие като нанасяне на много удари с ръце и крака, използване на тежки предмети и други външни влияния, които водят до болезнени усещания и травми. Според нея психологическото (емоционалното) насилие се заключава в заплаха, грубост, издевателство, оскърбление чрез думи или поведение предизвикващи отрицателна емоционална реакция и душевна травма. Самото емоционално оскърбление може да бъде идентифицирано много трудно, но както посочва Алексеева, то макар и да не оставя синини по тялото, може да бъде много по-разрушително от другото насилие. Сексуалното насилие е вид посегателство проявявано във форма на натрапчиви сексуални докосвания, сексуално унижение, принуждаване към секс и извършване на сексуални действия, включително и изнасилване въпреки нежеланието на жертвата. Икономическото насилие в семейството според посочената авторка се проявява като еднолично разпределение на средствата от семейния бюджет, строг контрол върху разходването на парите, и се проявява и като форма на емоционален натиск и оскърбление.

Домашното насилие наричано насилие в семейството включва в себе си посочените видове насилие. То се проявява не само в семейните двойки, но и при тези, които съжителстват на доброволни начала, при бивши съпрузи или между родители и деца, доказано е, че то не се ограничава в хетеросексуалните отношения [цит. по 3]. Доколкото домашното насилие е комплексен вид насилие, негова основна характеристика е, че независимо от формата на проявлението му то се повтаря като се увеличава честотата на цикъла на проявяването му. В някакъв смисъл авторите посочват, че това е система на поведение с помощта на която някой се стреми да съхрани властта и контрола над близкия си човек [цит. по 3]. По генезиса на разпространение

семейното насилие е разпространено във всички страни по света и сред всички слоеве на населението. Независимо, че има случаи на насилие на жени над мъже, то почестото явление (95% от случаите) е насилието на мъже над жени. Съществуват много и различни ситуации на проява на домашно насилие, като често срещано явление е жената, която живее в ситуация на насилие даже и да не разбира, че това което се случва с нея е проява на насилие [цит. по 3]. Както вече подчертахме случаите са достатъчно много, но в литературата се посочват такива [2], при които: партньора оскърбява и унижава жената; не й разрешава да се види с приятели и роднини; нанася побой или заплашва с побой; побой над децата; принуждаване на жената към секс против волята й; не пуска жената на работа; само той разпределя бюджета; постоянни критики към жената по отношение на това как изглежда, как се облича, как готви, как чисти и т.н.; внушава й чувство за вина пред децата и използва децата за опосредствено насилие. Това кара жената да се чувства безпомощна, ненужна на никому, да се страхува от партньора си, да вини само себе си и да живее подчинявайки се на чувството за дълг (Кораблина и др., 2001).

Често явление е жената да не намира в себе си сили да се раздели с партньора си. Като правило за това се изтъкват достатъчно причини от типа на: материална неосигуреност; невъзможност да се намери жилище; културно-исторически и религиозни и др. Към посочените причини авторите разглеждащи проблема [цит. по 3] сочат, че налице са огромно количество митове, като: идеята, че домашното насилие не е престъпление тъй като това е вътрешно семейна работа, или че на децата е нужен баща независимо от това, че той е агресивен, като най-популярен от тях е този, че жената трябва да бъде гъвката и да умее да се приспособява към мъжа си и ако не може да направи това, тя сама си е виновна. Към тези митове следва да причислим и една илюзия, която битува сред жертвите на насилие, а именно, че то е временно и повече няма да се повтори. За съжаление това не е така, в теорията за циклите на насилие се определят три фази или етапа, които се повтарят в разрушителни и разрушаващи взаимоотношения. Продължителността на всеки цикъл и тяхната периодичност варира във всеки отделен случай, но винаги се повтарят с нарастваща сила и честота [4]. Меновщиков (2002) прави следната характеристика на тези фази:

– първа фаза – нарастване на напрежението – проявяват се незначителни случаи на насилие, като удари и други при което нараства напрежението между партньорите. Пострадалите излизат от тази ситуация по различни начини: могат да отричат на насилието, могат да принизяват неговата значимост, но могат и трети сили да се намесят, за да контролират ситуацията и да я балансират. Характерно е, че жертвите на насилието оправдават жестокостта и даже защитават това поведение пред членовете на семейството и пред други хора;

– втора фаза – засилено насилие – към края на първата фаза се загубва контрола над процеса. В началото на втората фаза вече се проявява неизбежно другото насилие. Активната страна не е способна да управлява своето деструктивно поведение, което е начало и на терора в семейните отношения. Основна отличителна черта между двете фази е, че при втората и двете страни осъзнават, че ситуацията е излязла от контрол. Дори и жертвата да промени своето поведение, това не променя ситуацията;

– трета фаза – меден месец – фаза, която съдържа покой, любов, внимание и даже в някои случаи разкаяние. Жестокостта се сменя с подаръци, с добри мани-

ери, уверение, че това повече никога няма да се повтори, което кара жертвата да вярва, че насилието е приключено завинаги. Но доколкото самото взаимоотношение между партньорите е деструктивно фазата на медения месец завършва отново с преход към фазата на нарастване на напрежението, т. е. започва нов цикъл [4].

Мак-Клоски [цит. по 3] изследвайки семейното насилие в американското общество определя основните причини за неговата стабилност като проявление. Тя счита, че основния фактор за устойчивата проява на насилието са жените, които не са способни кардинално да променят ситуацията, да излязат от порочния кръг на насилствени взаимоотношения и по този начин да избавят себе си и своите близки от страданията. Тя също посочва наличието на пренос на вината от насилника върху жертвата. Посочва и икономически причини като парична зависимост, отсъствие на професия, образование, страх от понижаване на социалния статус, което кара жените доброволно да се самоизолират, да се страхуват от ревност и да демонстрират пълна преданост и самоотдаване в семейните отношения. Според нейните проучвания има много случаи, когато жената се подчинява на насилието, защото смята, че на мъжа по природа и по социално предназначение е присъщо да оскърбява и да държи съпругата си в страх. Характерно за нейните изследвания, че тя посочва, че голяма част от жените доброволно пренесли се в ролята на жертва в детството си са усвоили подобни стереотипи на поведение в своето семейство и поради това съзнателно се съгласяват на пълна зависимост от мъжа. Като правило това са жени с ниска самооценка, лишени от чувство за собствено достойнство на които им липсва усещане за ценността на собствения живот и поради това считащи, че напълно заслужават такова отношение. Вече споменахме, че преди всичко жените са жертва на семейно насилие, но ако и насилието над мъжете да не е разпространено толкова широко, то случаите не са редки и затова трябва да ги споменем и тях. Счита се, че не мъжете, а именно жените са носители и инициатори на насилието над децата, което в последствие прераства и в отношението към партньора. Не бива да се подценяват и случаите, когато и двамата партньори постоянно се провокират, уреждат си скандали, спорове, оскърбяват се и унижават един друг, които са случаи на така нареченото взаимно насилие. Както считат изследователите на подобни отношения [цит. по 3] не е важно кой ги инициира, отговорността в този случай носят и двете страни.

Не съществува единна теория, която да обясни напълно всички случаи и причини на домашно насилие. Ако вземем под внимание сложността на човешката природа, особеностите на социалното взаимодействие и характера на семейството като социална структура, освен това трябва да отчитаме и разнообразието на тези семейства, индивидуалните характеристики на техните членове и тези социални отклонения, които преплитайки се и съчетавайки се могат да породят насилие. Всичко това предава особено значение на взаимното влияние на хората един от друг и на постъпките, които предшестват или следват насилието. Това означава, че проблемите на домашното насилие независимо от своята острота и актуалност са многообразни като проявление, но са многообразни и от гледна точка на причините и етиологията им, а следователно и от гледна точка на практическата работа по тяхното предотвратяване или преодоляване [цит. по 3].

Ако се опитаме да направим портрет на потенциалните жертви на домашно насилие можем да кажем, че те проявяват следните признаци на поведение [цит. по 3]:

– изпитват страх от избухливостта на своя партньор;

– често отстъпват на партньора си боейки се да не оскърбят неговите чувства или да предизвикат гняв;

– изпитват желание да «спасят» партньора си когато той попада в неприятно или трудно положение;

– оправдават се пред себе си и пред другите, че имат лошо отношение към партньора;

– търпят ако партньора им проявява раздразнителност, злоба, блъска ги, бие ги и т. н.;

– вземат решение за своите действия или за отношението си към останалите в зависимост от желанието и оценката на партньора;

– оправдават партньора си с това, че той се държи точно така, както неговия баща е постъпвал с майка му.

Прието е да се смята (Меновщиков, 2002), че има определени черти на характера, които ако са налични при мъжете, почти със стопроцентова гаранция сочат за склонност към насилие [4]: ревност, желание за абсолютен контрол, склонност към бързи връзки, нереални очаквания, обвиняване другите за собствените проблеми, обвиняване другите за собствените чувства, хиперчувствителност, грубост към животните и децата, оскърбяване с думи, ригидни сексуални роли, случаи на насилие в миналото, заплаха от насилие, чупене на посуда и разрушаване на предмети, прилагане на сила в качеството на аргумент.

В заключение можем да кажем, че помощта на жертвите на домашно насилие се осъществява в специализирани институции (специални центрове за лица пострадали от домашно насилие; телефони на доверието; центрове за психологическа помощ; центрове за социална помощ и т.н.). Но можем да подчертаем, че помощта оказвана на пострадали от домашно насилие има своята специфика в зависимост от това кой я оказва (психолог, специалист по социална работа и др.), така й в зависимост от това на кого оказват помощта (вид на домашно насилие), и в каква форма оказват помощта (консултативна, психотерапевтична, социална поддръжка и т.н.). Можем да кажем, че болшинството автори се солидаризират с идеята, че последствията от семейното насилие се доближават до симптомите на посттравматично стресово разстройство. В чисто психологически план се набелязват следните стадии на терапия при работа с жертви на домашно насилие:

– вземане на решение за промяна – нужно е човек съзнателно да реши, какво е необходимо да се променя – задача на психолога е да създаде безопасно пространство и да оцени състоянието на психическо здраве на жертвата;

– криза – жертвата проявява силни чувства, преживява с болка всичко, което изисква от психолога много мощна поддръжка и практически ежедневни срещи;

– спомени – ако е създадено доверие към психолога би трябвало да последва разказ от страна на жертвата за това, което се е случило, като е много важно тя да преразкаже толкова, колкото психически може да издържи;

– вяра – ако човек се съмнява в точността на своите спомени, много е вярно да повярва в тях;

– преодоляване на мълчанието – подробен разказ за миналото вследствие на който жертвата преодолява вътрешната си изолация;

– сменане от себе си на вината за случилото се – за психолога е изключително важно помогне на клиента сам да снеме вината от себе си;

– разкритие и конфронтация – жертвата да преодолее страха си пред насилника и да разкрие своето истинско отношение към него;

– придобиване на духовност – възвръщане на представата за това, че света не е толкова лош и че в него има и добри хора;

– разрешаване на травмата и движение напред – момент, когато с помощта на психолога жертвата чувства, че й се е отдало отново да се включи в нормалния живот.

ЛИТЕРАТУРА:

1. Алексеева, Л. С. Психологическая помощь пострадавшим от семейного насилия: Научно-методическое пособие – М.: ГосНИИ семьи и воспитания, 2000
2. Кораблина, Е. П., Акиндинова И. А., Баканова А. А., Родина А. М. Искусство исцеления души: Этюды о психологической помощи: Пособие для практических психологов. СПб., 2001
3. Малкина-Пых, И. Г. Экстремальные ситуации. М., 2006
4. Меновщиков, В. Ю. Психологическое консультирование. Работа с кризисными и проблемными ситуациями. М., Смысл, 2002

ЗА СУИЦИДНОТО ПОВЕДЕНИЕ

Красимир М. Марков

Шуменски университет „Епископ Константин Преславски”
Педагогически факултет

OF SUICIDAL BEHAVIOR

Krasimir M. Markov

ABSTRACT: *Discussed psychological problems suitsidalno the expression of the manifestation of behavior and the factors influencing its origin*

KEY WORDS: *psychology, suicide factors arise*

Откакто човечеството съществува винаги е имало хора, които са се лишавали от живот по собствено желание. В много от тези случаи причината за това е тежко заболяване с фатален край, което доведе до възникване на широко дискутирания проблем за евтаназията и разрешаването й в някои страни. Доколкото проблема за евтаназията е проблем свързан с предотвратяване на тежки, нежелани от лицето прояви на заболяване и доколкото моралността на този акт все още широко се дискутира на този проблем няма да се спираме. Съществуват обаче много суицидни явления продиктувани от други проблеми, явяващи се фактори за генезиса на подобно поведение на които ще се спрем по-късно. Независимо от това отсега

може да се коментира, че в общества преживяващи тежки социални, икономически и други кризи броя на самоубийствата се увеличава значително.

По принцип под самоубийство (суицид) се разбира съзнателно да се лишиш от живот. Проблемът за суицидалното поведение е малко по-широк. Някои автори [4] считат, че то включва в себе си суицидални покушения, опити и прояви (Кондратенко, 1999). Към покушенията се отнасят всички суицидални опити незавършили със смърт по причина независещa от самоубиеца. Към суицидалните прояви се отнасят съответните мисли, изказвания, намеци, които обаче не се съпровождат с действия към лишаване от живот. Кондратенко (1999) прави и друга класификация разделяща самоубийственото поведение на – самоубийства (истински суициди); парасуициди (актове на целенасочено самоповреждане недовеждащи до смърт) и пресуициди (състояние на личността, което се обуславя от повишена норма на вероятност за прибягване към суицидален акт).

Обикновено в литературата [16] феноменът на суицида се свързва с представата, че личността посягаща на себе си е в състояние на психологическа криза, като под криза се разбира емоционално състояние възникващо в ситуация на сблъсък на личността с препятствия възникващи по пътя на удовлетворяването на нейните жизнени потребности. В случая се разбират такива препятствия, които не могат да бъдат преодолени с нормалните методи и средства, с които си служи личността в живота(Farberow, 1980). Други автори [2] считат, че психологичната криза предизвиква фрустрация на важни потребности в индивида и специфична личносттна реакция към тази фрустрация (Абрумова, Тихоненко, 1980).

Съгласно социологическата теория на самоубийството разработена от Дюркхайм [3] суицидалните мисли се проявяват преди всичко когато има разрив в интерперсоналните връзки на личността, в смисъл на отчуждение на индивида от тази група към която принадлежи. Според посочения автор има три основни вида самоубийства:

– егоистично саморазрушение – обусловено от факта, че индивида се чувства отчужден и изолиран от обществото, семейството и приятелите;

– аномично самоубийство – появява се в следствие на трудности в приспособяването на човек към измененията в обществото довеждащо до нарушаване на връзките на човека със социалната група;

– алтруистично – това е самоубийство, което се извършва от човека, ако авторитета на обществото или групата подавят неговата егоидентичност и той се жертва за благото на обществото или заради някаква социална, религиозна, или философска идея (Дюркхайм, 1994).

Австрийския психиатър Зигмунд Фройд развива представа за самоубийството основана на идеята за двете основни влечения на човека: Ерос – влечение към живота и Танатос – влечение към смъртта. Според него целия човешки живот представлява битка между тези две влечения, в смисъл, че човек иска да живее, да бъде обичан, да продължава себе си в своите деца, но има и периоди в които желана се оказва смъртта. Той счита, че с възрастта силата на Ерос намалява, а Танатос увеличава своята сила и става все по-напорист. В този смисъл Фройд твърди, че и суицида, и убийството се явяват проява на разрушителната сила на Танатос и в този смисъл са агресия (цит. по Моховников, 2001).

Алфред Адлер основавайки индивидуалната психология развива идеята, че да бъдеш човек означава преди всичко да усещаш преди всичко собствената си не-

пълноценност. Живота на човека според него се състои от това, че се стреми към цели, които могат да не се осъзнават, но направляват нашите постъпки и формират нашия жизнен стил. По подобие на Дюркхайм и Адлер твърди, че за човека е изначално важно да усеща общността с другите хора. Затова и в течение на живота на човека той се намира в състояние на търсене на начини за преодоляване на комплекса за непълноценност и за неговата компенсация, или свръхкомпенсация. Ако в хода на това търсене на начини за преодоляване на комплекса човек се натъкне на значително препятствие и в този смисъл се формира кризисна ситуация, човек започва така нареченото бягство в самоубийството. Загубва се чувството за общност между човека и обществото, установява се дистанция, в сферата на емоциите възниква ярост, ненавист и чувство за мъст. Адлер счита, че доколкото на човека е свойствен вътрешен стремеж към целта, в повечето случаи безсъзнателен, то ако знаем последователността на неговите постъпки в случай на автоагресия тя може да бъде предотвратена.

К. Менинджър (1985, 1991) като последовател на психоаналитичното направление развива идеята на Фройд за самоубийството като изследва неговите дълбочинни мотиви. Той определя три съставни части на суицидното поведение [17]:

– желание за убийство – самоубийците бъдейки в повечето случаи инфантилни личности реагират яростно на пречките или пепятствията стоящи на пътя реализацията на техните желания;

– желание да бъдеш убит – ако убийството се явява крайна форма на агресия, то суицида сам по себе си представлява висша форма на подчинение, човекът не може да издържи упреците на съвестта и страданията, които му причинява нарушаването на моралните норми, поради което вижда изкупването на своята вина единствено в прекратяване на собствения живот;

– желание да умреш – разпространена е сред хора, които са склонни да подлагат своя живот на необснован риск, а също така сред болни, които смятат смъртта за единственото избавление от соматични и душевни мъки.

Менинджър счита, че ако у човек възникнат тези три описани желания суицида се превръща в непредотвратима реалност, а ако тези желания се размият във времето се проявяват по-меки форми на автоагресивно поведение.

Разглеждайки проблемите на самоубийството К. Юнг сочи, че причина за суицид може да стане безсъзнателния стремеж на човека към духовно прераждане. Този стремеж е обусловен от актуализация на архитипа на колективното безсъзнателно, което приема различни форми [14]:

– метемпсихоза – преселение на душата – когато живота на човека преминава през различни телесни въплъщения;

– превъплъщение – предполагащо съхраняване на непрекъснатостта на личността и ново раждане в човешкото тяло;

– възкресение – възстановяване на човешкия живот след смъртта във формата на т. нар. тънко тяло;

– възраждане – възстановяване в пределите на индивидуалния живот с превръщане на смъртното същество в безсмъртно;

– възраждане по пътя на трансформацията протичаща вън от личността.

Развивайки идеите на психодинамичното направление и егопсихологията К. Хорни [цит. по 6] смята, че при нарушение на взаимоотношенията между хората възниква невротичен конфликт породен от така наречената базисна тревога, според

нея тя се проявявав още в детството поради усещане на враждебността на обкръжението. Освен тревожност в невротична ситуация човек се чувства самотен, безпомощен, зависим и враждебен. Тези феномени могат да станат основа на суицидално поведение. К. Хорни смята, че враждебността при конфликта актуализира разрушителни наклонности насочени към самия себе си. Те не са свързани непременно със суицидално поведение и могат да се проявят във вид на презрение, отвращение или глобално отрицание, те се усилват ако външните трудности се съчетаят с егоистичните нагласи или илюзии на човека. В такъв случай враждебността и презрението към себе си и другите могат да станат толкова силни, че собствената смърт да стане привлекателен способ за отмъщение. Покоряването на съдбата, при което автодеструктивността се явява преобладаваща тенденция се разглежда от Хорни като латентна форма на самоубийство.

Развивайки теорията си за междуличностното общуване Х. Съливан [цит. по 6] разглежда самоубийството в светлината на самооценката на индивида, която се създава по пътя на преценката на отношенията на другите хора към него. В резултат на тази самооценка у човек могат да се формират три Аз-образа:

– «добро Аз» - ако отношението на другите осигурява нашата безопасност;

– «лошо Аз» - ако обкръжението поражда тревога или други емоционални нарушения;

– «не Аз» - възникващо, когато човек загубва егоидентичността си, както се случва при душевни разстройства или суицидални ситуации.

Ако човек съществува в състояние на жизнени кризи или междуличностни конфликти той вегетира продължително в състоянието на «лошия Аз», който се явява източник на жизнен дискомфорт. В този случай прекратяването на страданията по пътя на извършване на автоагресия и по-точно превръщането си в «не Аз» става приемлива или единствено възможна алтернатива. Според Съливан чрез суицидния акт човек едновременно заявява и своята враждебност към другите хора и към целия свят.

Представителите на хуманистичната психология Р. Мей и К. Роджърс подчертават ролята на тревогата и другите емоционални преживявания за развитието но суицидално поведение. Р. Мей [цит. по 6] счита, че тревогата се явява не само симптом, но и екзистенциално проявление на живота и важна конструктивна сила в човешкия живот. К. Роджърс [8] смята, че основната тенденция на живота се състои в актуализацията, съхранението и засилването на Аз-а формиращо се във взаимодействие със средата и другите хора. Ако структурата на Аз-а е ригидна, то несъгласуващия се с нея реален опит се възприема като заплаха за живота на човека.

Виктор Франкъл [11] разглежда самоубийството заедно с такива понятия като смисъл на живота, свобода на човека, а също така и във връзка с психологията на смъртта. Франкъл счита, че самоубиецът не се бои от смъртта, а се бои от живота.

Независимо, че посочените автори описват идеята за суицидално поведение за първи път Е. Шнейдман (2001) описва признаците, които свидетелстват за приближаването на самоубийството като ги нарича ключове към суицида. Създавайки оригинална типология на индивидите, които съзнателно се приближават към смъртта той ги класифицира като[13]:

– търсачи на смъртта – целенасочено търсещи раздялата с живота, свеждащи възможностите за спасение до минимум;

– инициатори – целенасочено приближаващи се към нея в случай на тежка болест като прекратяват да се хранят, да вземат лекарства и т.н.;

– играчи със смъртта – склонни да търсят ситуации, в които живота се счита за залог, а възможността за оцеляване има ниска вероятност;

– одобряващи смъртта – тези, които не се стремят активно да се разделят с живота, но взаимно с това не скриват своите суицидни намерения.

Шнайдман описва и определя общите черти характерни за всички самоубийци без значение от обстоятелствата и методите на извършване на самоубийството[13]:

– обща цел за самоубийците се явява търсенето на решение;

– обща задача на самоубийците е прекратяването на съзнанието;

– общ стимул за тях е непоносимата психична болка;

– общ стресор са фрустрираните психологични потребности;

– обща суицидална емоция е безпомощността и безнадеждността;

– общо вътрешно отношение към самоубийството е амбивалентността;

– общо състояние на психиката при суицида е свиването когнитивната сфера;

– общо действие при суицида е бягството или агресията;

– общо комуникативно действие при суицида е съобщаването за своето намерение;

– обща закономерност на суицидното поведение е общия стил на поведение в продължение на целия живот.

Амбрумова (1991) правейки характеристика на суицидалното поведение определя шест типа ситуационни реакции [2]:

– реакции на емоционален дисбаланс – характеризират се с отчетливи промени в гамата на дистимичните изменения. Общия фон на настроението е сменен и човек усеща в по-голяма или по-малка степен дискомфорт. Характерно е плавното повишаване на нивото на тревожност;

– песимистични реакции – проявяват се на първо място в промяна в мирогледа, който придобива мрачна украска със съответстващите съждения и оценки, и промяна и преструктуриране на системата на ценностите;

– реакции на отрицателния баланс – проявяват се като рационална равносметка на преминалия живот и формулиране на съответните изводи;

– реакция на демобилизация – тя се характеризира с най-резки изменения в сферата на контактите заключаващи се в отказ от обичайните контакти или значителното им ограничаване;

– реакция на опозиция – характеризира се с повишена степен на агресивност и нарастваща рязкост на отрицателните оценки към околните и тяхната дейност;

– реакция на дезорганизация – почива на основата на тревожния компонент.

Соловьова (2001) описва пет вида суицидално поведение в съответствие с доминиращите мотиви [10]: протест; молба за състрадание; избягване на физическите или душевни мъки; самонаказание; отказ от живота.

Определено е ясно, че за проявата на суицидално поведение влияят различни по сила и интензиност фактори. Независимо, че тяхното изброяване е достатъчно

условно доколкото самото им влияние се преценя от човека субективно, бихме могли условно да преведем някои от факторите на суицидален риск [цит. по 6]:

Социално-демографски фактори:

– възраст – суицидални актове се срещат във всяка възрастова група като има данни за опити за самоубийства при деца на възраст между 3 и 6 години, независимо, че суицидално поведение при децата до 5 години се среща изключително рядко. **Първия** пит на суицидална активност се среща във възраст между 15 и 24 години, което е свързано с високите изисквания, които тази възраст предявява към адаптационните механизми на личността. **Втория** пит е във възрастта между 40 и 60 години, тъй като освен психологическите проблеми за тази възраст е характерно влошаване на телесното здраве, хормонално пренастройване, промяна на йерархията в ценностите, което често се съчетава с депресия. Всъщност депресията е най-често срещаното психично разстройство през този период. При това в тази възраст се случва обстоятелства свързани със събития като това, че порасналите деца напускат дома си, възрастните родители почиват, а най-често съществуват и проблеми в професионалното развитие. **Третия** пик на суицидален риск е при възрастните хора, при което той е четири пъти по-голям, отколкото в цялата популация;

– пол – жените по-често извършват опити за самоубийство, при които избират по-малко мъчителни и болезнени начини, отколкото мъжете, а при мъжете самоубийството носи завършен характер. Ако сравним количеството опити за самоубийство между жените и мъжете, то съотношението е 2 – 3 към 1 в полза на жените, но по количеството извършени самоубийства и нанесени телесни повреди мъжете превъзхождат жените;

– образование и професия – по-често самоубийства извършват безработните или лицата с висше образование и висок професионален статус. В изследване проведено в Русия през 1994 Кащан и Седок привеждат данни, според които най-висок е суицидалния риск при лекарите сред които на първо място са психиатрите, след тях са офталмолозите, анестезиолозите и дентисти. В рисковата група влизат музикантите, юристите, младшите офицерски чинове и застрахователните агенти. Най-нисък е суицидалния риск при лицата със средно образование и среден социален статус;

– местожителство – количеството самоубийства е по-високо сред градските жители, като е забелязана закономерност на право пропорционална зависимост между плътността на населението и честотата на самоубийствата;

– семейно положение – едно от най-значителните влияние върху суицидалния риск оказва семейното положение и особеностите на вътрешносемейните отношения. По принцип живеещите в семейство по-рядко извършват самоубийство, отколкото несемейните, разведените или с починали съпрузи и съпруги. Практиката показва, че съществува определена градация на риска в зависимост от семейното положение: най-рискова е групата е на тези, които никога не са създавали семейство; след тях е групата на овдовелите и разведените; след които са семействата без деца и накрая тези семейства, които имат деца. Доказано е също така, че сред суицидите преобладават лица, които са отгледани от приемни родители, възпитани в интернати и други такива заведения или имащи само един родител. Съществено влияние оказва и социалнопсихологическия тип на семейството. Най-рискови за суицид са семейства при които отсъства емоционална и духовна сплотеност, нямат единни цели и потребности, отсъства мотивация за съвместен живот,

или такива, които се характеризират с корпоративност – при тях задълженията на член от семейството се изпълняват само при условие, че другите членове на семейството имат същите задължения; консервативни – неспособност на членовете на семейството да запази наложената комуникативна структура под влияние на външни авторитети; закрити – които съществуват в затворена среда и членовете на семейството имат ограничени социални контакти.

– социално-икономически фактори – Световната здравна организация дава данни според, които честотата на самоубийствата е право пропорционална на степента на икономическото развитие на страната. Доказано е също така, че в периоди на войни и социални вълнения (въстания и революции) нивото на самоубийствата значително се намалява, а при икономически кризи се увеличава;

– биографични фактори (предложени са от Ромек 2004): хомосексуална ориентация – при нея честотата на самоубийствата е по-голяма при тийнейджърите от двата пола и при възрастните мъже; наличие на суицидални мисли, намерения и опити в миналото; суицидално поведение на роднини, приятели или други значими лица в това число религиозни, политически лидери и кумири в областта на спорта, музиката и т. н. [9].

Индивидуално-психологически фактори:

Личностните и характерологичните особености често играят водеща роля при формирането на суицидално поведение. Независимо от това опитите да се направи връзкъ между отделните черти на личността и готовността за самоубийство не са дали резултати [цит. по 6]. Приема се, че решаващо влияние в опитите за суицидално поведение вероятно имат не конкретните личностови характеристики, а цялостната структура на личността и балансирането на нейните съставящи. Различните автори преекспонират различни фактори влияещи върху суицидалното поведение: психолого-психиатрични (Короленко, Донских 1990) – повишена напрегнатост, стремеж към емоционална близост, импулсивност, чувство за вина, хипореактивност и др.; акцентуации на характера (Кличко 1977, Юрьева 1999) – при циклоиден, емоционално лабилен, епилептоиден и стероиден тип; личностен стил (Моховников 2001) – импулсивен, компулсивен, рискуващ, репресивен, зависим, амбивалентен, отричащ, гневен, обвиняващ, избягващ, безчувствен, захвърлен, творчески.

Медицински фактори – психическо здраве – следните диагностични категории: психически здрави, лица с гранични психични разстройства, психично болни; соматично здраве – наличие на тежко хронично прогресиращо заболяване;

Природни фактори – забелезян е преимуществен риск на самоубийствата през пролетта. Има опити да се установи зависимостта на честотата на самоубийствата от деня на седмицата, като се смята, че по-често са в понеделник, а към края на седмицата намаляват. И от времето на денонощието по-често вечер, в началото на нощта или в ранното утро. Но данните за природните фактори са противоречиви, изследвани с в това число зависимостта от географската ширина, фазите на луната, земния магнетизъм, количеството слънчеви петна, но не е открито влияние върху суицидалното поведение.

В заключение можем да кажем, че съществуват определени индикатори отчитащи възможността от суицидален риск. Те се подразделят в следните групи [цит по 6]: ситуационни индикатори, поведенски индикатори, комуникативни индикатори, когнитивни индикатори, емоционални индикатори. Държейки сметка за на-

личието на действия на който да било от тези индикатори или на някаква тяхна съвкупност, бихме могли да прогнозираме и в определени случаи да попречим на проявите на суицидално поведение.

ЛИТЕРАТУРА:

1. Адлер, А. Практика и теория индивидуальной психологии / Пер. с нем. М., Прогресс, 1995
2. Амбрумова, А. Г., Тихоненко В. А. Диагностика суицидального поведения: метод, рекомендации. М., 1980.
3. Дюркгейм, Э. Самоубийство. Социологический этюд / Пер. с франц. М., Мысль, 1994.
4. Кондратенко, В. Т. Суицидальное поведение // Психология экстремальных ситуаций: Хрестоматия / Сост. А. Е. Тарас, К. В. Сельченок. Минск, Харвест, 1999.
5. Конончук, Н. В. О психологическом смысле суицидов //' Пси- і хологический журнал, 1989. Т. 10. № 5, с. 96–102. |
6. Малкина-Пых, И. Г. Экстремальные ситуации. М., 2006
7. Моховиков, А. Н. Введение к клинико-психологическому разделу // Суицидология: прошлое и настоящее. Проблема самоубийства в трудах философов, социологов, психотерапевтов и художественных текстах / Сост. А. Н. Моховиков, М.: Когито-центр, 20016
8. Роджерс, К. Р. Консультирование и психотерапия. Новейшие подходы в области практической работы. М., 1999.
9. Ромек, В. Г. Конторович В.А., Крукович Е.И. Психологическая помощь в кризисных ситуациях. СПб., Речь, 2004
10. Соловьева, С. Л. Психология экстремальных состояний. СПб., ЭЛБИ, 2003
11. Франкл, В. Психотерапия на практике. СПб., Ювента, 1999
12. Хорни, К. Невротическая личность нашего времени. Самоанализ. М.. Мысль, 1994.
13. Шнейдман, Э. Десять общих черт самоубийств и их значение для психотерапии // Суицидология: прошлое и настоящее. Проблема самоубийства в трудах философов, социологов, психотерапевтов и художественных текстах / Сост. А. Н. Моховиков. М., Когито-центр, 2001
14. Юнг, К. Г. Душа и миф: шесть архетипов / Пер. с англ. Киев: Гос. б-ка Украины для юношества, 1996.
15. Ясперс, К. Общая психопатология. М., Практика, 1997.
16. Farberow N. L. The many faces of suicide. – New York, 1980.
17. Menninger K. Man Against Himself. A Harvest/ HBJ Book, Harcourt Brace Jovanjvic Publishers. – San Diego, New York, London, 1985.
18. Menninger, W. Identifying, evaluation, and responding to boundary violations: A risk management program // Psychiatric Annals, 1991, vol. 21(11).

ПСИХОЛОГИЧЕСКИ АСПЕКТИ НА КОРПОРАТИВНАТА СИГУРНОСТ ПРИ ВОДЕНЕ НА ПРЕГОВОРИ

Красимир М. Марков

Шуменски университет „Епископ Константин Преславски”
Педагогически факултет

PSYCHOLOGICAL ASPECTS OF CORPORATE SECURITY DURING BARGAINING

Krasimir M. Markov

ABSTRACT: *Describe the psychological aspects and their importance in the conduct of negotiations corporate security organization*

KEY WORDS: *psychology*, negotiation, organization, security

Воденето на преговори е важна съставна част от живота на всяка една организация. В крайна сметка те представляват общуване между двама или повече хора, представляващи интересите на независими една от друга страни с цел да се изработи взаимоприемливо решение по въпроси имащи важно значение за всеки от участниците [виж 1]. Преговорите могат да се провеждат както еднократно, така и в хода на много срещи между участниците, при които да се уточнят определени детайли на търсеното решение. Като правило в края на преговорите се излиза със съгласувано споразумение между страните. Напълно естествено е, че в хода на тези преговори всяка от страните отчита юридическите и икономическите зависимости в които се намира с другата страна. Ако те не бъдат отчитани преговорите се превръщат в друга форма на общуване – съвещание, инструктаж, събеседване и т.н.

Истинските преговори се провеждат по определен алгоритъм и изискват специална подготовка. Ако може изобщо да се приведе идеална схема за провеждане на преговори, тя би могла да се представи в следния вид [по 1]:

Предварителен етап:

Отчитане на факторите определящи параметрите на модела:

- цел на преговорите (програма минимум и програма максимум);
- отчитане на собствените сили и средства;
- отчитане на степента на осведоменост за потенциалните възможности на другата преговаряща страна.

Създаване на рефлексивен модел на преговорите (модел на виждане на преговорите от гледна точка на другата страна в тях). Тук има позиции, които също трябва да бъдат разгледани:

- мотивация на участващите в преговорите и очаквани резултати;
- сили и средства, които другата страна може да използва в хода на преговорите;

– ниво на осведоменост на другата страна за нашите ресурси, възможности, планове и цели.

План на преговорите.

Когато се провеждат преговори един от важните въпроси за който се държи сметка е да има предварително набелязан план за тяхното осъществяване. Обикновено в литературата се посочват следните раздели на плана:

– процедурни въпроси (място и време на провеждането на преговорите, разположение на участниците в залата за преговори, дрескод, присъствие на помощен персонал, наличие на безалкохолни, кафета и т.н.);

– информационно осигуряване (определяне какви документи основни и резервни ще бъдат необходими за преговорите и тяхното възможно използване в различните фази на преговорите);

– състава на участващите в преговорите от двете страни;

– техническо осигуряване (мултимедия, аудиовизуални техники и т.н.).

Репетиция за преговорите.

Уважаващите себе си организации в случай, че преговорите които предстоят са от съществено значение за успешното развитие на организацията провеждат репетиции, които се заключават в следното:

– инструктаж на участниците – лицата участващи в преговорите се запознават с основните позиции в плана за преговорите и задачите, които ръководството на организацията е поставило като цели за достигане в преговорите;

– репетиция – заключава се в проиграване на линията на поведението на всеки от участниците и на екипа участващ в преговорите като цяло.

Преговори:

Начало на преговорите – основната същност на тази фаза е идеята да се установи психологически контакт между участниците. За целта могат да се използват прийоми като:

– разкриване на възможните психични бариери на общуването и търсене на пътищата за тяхното премахване;

– преценка на партньорите по преговорите (оценка на водещите мотиви на партньорите);

– определяне на стратегията за вземане на решение;

– преценка на подбраните вербални и невербални сигнали;

– проверка на ефективността на подбраните методи за привличане на партньора по преговори.

Основна част на преговорите. По принцип тя се заключава в:

– уточняване предмета на преговорите и преглед на обсъжданите въпроси;

– определяне на позицията на страните с основно внимание на изясняване на мнението на всеки участващ в преговорите от противниковата страна;

– търсене на пътища за сближаване на позициите в процеса на обсъждането започвайки с най-малко значимите.

Изводи от преговорите.

Всяка страна участваща в преговори в резултат от тяхното приключване трябва да си направи изводи целящи усъвършенстването на действията си при провеждане на следващи преговори. Най-общо тези изводи биха могли да се определят в два плана:

– обща оценка на резултатите от преговорите;
– оценка на действията на всеки от участниците в преговорите.

Естествено е, че воденето на преговори освен постигането на крайните цели на организацията или поне търсене на оптимално сближение на позициите на двете преговарящи страни, има аспекти за които също трябва да се държи сметка при организацията и воденето на преговорите. Един от тези аспекти е сигурността на организацията, което означава преговорите да се водят така, че важните проблеми да се разискват без да се понижава нивото на корпоративната сигурност. За тази цел служи и другия аспект на преговорите – тяхната психологическа страна.

Психологическата страна на преговорите има голямо значение от гледна точка на идеята за снемането на психичните бариери възникващи в хода на преговорите. В този смисъл е необходимо да бъдат използвани определени методи на психологическо въздействие. Тези методи могат да бъдат наречени както методи на управление на преговорите, така и методи на манипулация.

Един от тези методи е внушението. Внушението е едно от средствата за взаимно влияние на хората в процеса на общуването. При него за разлика от внушението под хипноза или сън е характерно, че то се осъществява не безсъзнателно и безкритично, а само със занижена степен на критичност. За различните хора е характерно, че имат различна степен на внушаемост. Нещо повече, тази степен на внушаемост не е постоянна даже при един и същи човек, и зависи от:

– характера на социалната роля – доказано е, че при промяна на социалната роля в низходяща позиция се засилва степента на внушаемост на човека, и обратно;

– възрастта – младите хора по-лесно се поддават на внушаемост, отколкото хората в зряла възраст, което се обуславя от по-големия социален опит;

– културното ниво – културното ниво също е свързано със социалния опит, съвсем естествено е, че хората отраснали в културна и информирана среда ще са по-малко внушаеми от тези, които растат в по-ниско културна и по-малко информирана среда. Културното ниво е свързано и с образователното, което влияе върху внушаемостта по същия начин;

– пола – жените са по-внушаеми от мъжете, но има една особеност, ако жената играе лидерска роля нейната внушаемост се понижава;

– типа нервна система – така наречения мислителен тип е по-малко внушаем, отколкото емоционалния;

– моментното психично състояние – при повишена тревожност или стресово състояние внушаемостта се повишава;

– условия – когато казваме условия имаме предвид изкуствено създавани такива с помощта на които бихме могли да усилим внушаемостта над другата страна в преговорния процес (обстановка, осветление, начин на говор и т.н.).

Начини и прийоми за провеждане на внушението има различни, но общо взето най-често се използват прякото и косвеното внушение. Прякото внушение е внушението, което се отправя във вид на съвет или предложение, но този прийом е ефективен само ако другата страна в преговорите изпитва достатъчно доверие към партньора в преговорите. Това невинаги е възможно и е трудно постижимо, поради което по-често се използва косвеното внушение. То може да бъде използвано във форми като:

– намек – при него се обръщаме не към съзнанието на обекта на внушение, а към неговите чувства и емоции;

– косвено одобрение – косвеното одобрение разчита на положителното емоционално възприятие в ситуация, когато подбуждаме партньора по преговорите към действие, и в този смисъл има доста добър внушаващ ефект;

– косвено осъждане – при него се разчита на формиране на негативни емоции в ситуация на подбуждане на партньора по преговорите към отказ от участие в действие;

– ефект-плацебо – преписване на неутрално средство магическо въздействие;

– обходен маньовър – довежда се противниковата страна в преговорите до идеята, че предлаганото решение е плод на нейните разсъждения;

– излъгано очакване – обектът на внушение очаква една информация, а всъщност получава съвсем друга;

– метод Сократ – на внушаемия се задават серия въпроси на които той трябва да отговаря само с „да". В края на серията от въпроси се поставя значимия за нас, на който той по инерция отговаря с „да";

– взрив – заключава се в неочаквано използване на информация изцяло променяща ситуацията на преговорите.

Заключение при описване на внушението. Можем да кажем, че то има най-добър ефект, ако информацията която предлагаме е личностно значима за обекта на внушение или е насочена към формиране на противоположни нагласи.

Друг от тези методи е убеждението. Той представлява такава форма на психологическо въздействие при която информацията се довежда до съзнанието на обекта с цел да го подбуди към вземане на необходимото решение. Като правило убеждението може да бъде няколко вида:

– информиране – довеждане на информация до знанието на обекта без коментари;

– разяснение – информацията се съпровожда с коментар;

– схематично убеждение – информацията се поднася във вид на определена логическа последователност;

– разсъждаващо убеждение – информацията се съпровожда с коментари и разсъждения за различните варианти на развитие на ситуацията;

– проблемно – информацията се поднася във форма на описание на проблемна ситуация изискваща решение от обекта на въздействие;

– убеждение-доказателство – форма на убеждаващо въздействие изискваща построение на въздействието в строга система от причинно-следствени връзки в съответствие със законите на логиката.

Принуждение. Принуждението е третата форма на психично въздействие в хода на преговорите. При нея обектът е принуден да приема поставените му условия независимо от своето нежелание. Обикновено то се осъществява в следните форми:

– забрана – ултимативно условие принуждаващо обекта да се откаже от реализацията на взетото решение;

– предупреждение – информиране на обекта за нежелани за него последствия в случай, че продължава избраната форма на поведение;

– заплаха – предупреждаване на обекта за прилагане на санкция в отговор на неговите действия.

Всеки от обсъдените методи на психично въздействие може да бъде използван или като управляващо въздействие, или като манипулативно въздействие. Ако на партньора в преговорите се предоставя максимално пълна и достоверна информация, тя му позволява да вземе правилно осмислено решение, в такъв случай говорим за управляващо въздействие. Но ако информацията съдържа в голяма степен недостоверност или е изкривена, то тогава другата страна е принудена да вземе това решение, което усилено й се подсказва. Тогава говорим за манипулативно въздействие.

Когато използваме методите на психологическо въздействие за манипулация, практиката показва, че могат да бъдат използвани многочислени уловки. Обикновено такива са:

- отхвърляне на възраженията;
- шок;
- рязко излизане от дискусията;
- представяне на лъжливи тези;
- подмяна на предмета на дискусията;
- инсинуации;
- отвличане на вниманието;
- изваждане от равновесие;
- подмяна на пунктовете на разногласие.

Разгледаните проблеми на психологическо осигуряване на корпоративната сигурност при водене на преговори има условен характер. В крайна сметка в реалността съществува някакво поле на взаимодействието между векторите на заплаха и векторите, които противодействат на заплахата. Това взаимодействие протича на различни нива и по различни механизми. Само едно от тези нива всъщност е психологическото, механизмите на което се явяват законите на функционирането на човешката психика.

ЛИТЕРАТУРА:

1. Бородин, И. А. Основы психологии корпоративной безопасности. М., 2004
1. Виханский О. С. Стратегическое управление. М., 1995.
2. Петров, А. Н. и др., Стратегический менеджмент. Питер СПб. 2005
3. Портер, М. Международная конкуренция. МО, М. 1993
4. Стратегическое планирование /Под ред. Э. А. Уткина. М., 1998.
5. Томпсон А. А., Стрикленд А, Дж, Стратегический менеджмент. М., 1998.
6. Тренев Н. Н. Стратегическое управление. Уч. пос. М., 2000.
7. Chang Y. N., Campo-Flores F. Business Policy and Strategy, Text and Cases. Good year Publishing Company. — Santa Monica, 1980.
8. Greenly G. E. Strategic Management. — Prentice Hall, London, 1989.
9. Jonson G., Scholes K. Exploring Corporate Strategy. An Aproach to Strategic Management. — Pitman, London, 1992.
10. Mintzberg H. Power in and around organizations. N.Y., 1983.
11. Robey P., Sales A. Designing organizations. Burr, 1996.
12. Rowe A., Mason R., Dickel K. Strategic management. N.Y., 1996.
13. Rowe A., Mason R., Dickel K., Snyder N. Strategic management: a methodical pproach. N.Y., 1989.

СПЕЦИФИКА НА МИГРАЦИОННИТЕ ПРОЦЕСИ В ЕВРОПА ПРЕЗ XXI ВЕК

Чавдар Л. Милков

Община „Търък“, Англия, Дирекция „Социално подпомагане“

SPECIFICS OF THE MIGRATION PROCESSES IN EUROPE IN THE 21-TH CENTURY

Chavdar L. Milkov

ABSTRACT: *Present day migration processes and the consequences from them have established as one of the major aspects of the European Union immediate and pressing politics. In the era of globalisation, migration has become one of the primary topics for discussion. This makes it a challenge, requiring conceptual resolutions at all levels - from a strategic to a local.*

KEY WORDS: *Migration, migration processes, reasons for migration, refugees.*

Въведение

Миграцията на населението е един от най-важните проблеми на народонаселението и се разглежда не само като просто механично придвижване на хората, а като изключително сложен и деликатен процес, засягащ много аспекти: социално-икономическия, обществено-политическия, етно-националния, нравствено-психологическия, образователно-възпитателния, религиозно-духовния начин на живот на цели страни и народи. Повече от 3% от жителите на Земята, в момента, са със статут на мигранти. Към тях трябва да прибавим и няколко десетки милиона търсещи убежище, бежанци и изгнаници.

Модерните миграционни процеси и техните последици с основание са се наложили като едно от централните полета на актуалната политика в Европейския съюз. Векове наред самата Европа е континент на емигранти, като жителите на европейските държави колонизират обширни пространства по всички останали континенти, търсейки богатство, свобода, просперитет и мир. Днес тенденцията е обърната: в епохата на агресивната, настъпателна и повсеместна глобализация Старият континент се е превърнал в крайна цел на непознати досега, по мащаба и интензивността си, миграционни процеси. Класическият „Push-and-Pull“- модел на пръв поглед тук е лесно приложим: от една страна фактори, като бедност, липса на перспективи, пренаселване, войни, репресии, природни катаклизми и т. н., мотивират жителите на слаборазвити или развиващи се страни да емигрират за да потърсят нов живот другаде. От друга страна, Европа страда от чувствително застаряване на населението, както и от липса на квалифицирани работници. Тези процеси поставят под въпрос приеманите досега като подразбиращи се постижения: социалната държава, благосъстоянието и конкурентоспособността на европейските икономики в глобален план. За да може да ги поддържа, ЕС се нуждае от сериозен

човешки ресурс, който обаче не може да си осигури сам. В този смисъл, може да се заяви, че миграционните процеси към Стара Европа, дори при повърхностен поглед върху проблема, са безалтернативно явление, което, до голяма степен, вече формира бъдещето на нашия континент.

I. Насоки на изследователската дейност, свързана с миграционните процеси в Европа

Ролята на изследователите и научните работници е особено ценна в следните области:

1. Проучване на външните и вътрешни причини за появата на миграционните потоци, основните й пътища, фактори, движещи сили. Необходимо е точно и конкретно отчитане на открояващите се миграционни тенденции в света, и по-специално, в Европа през XXI век, в техните специфични, транскултурални и глобализационни измерения.

2. Анализ на степента на въздействие на миграцията върху приемащите страни и страните на произход, както от социално-икономически, така и от културален характер. Според Хр. Попов, е наложително „изчисляването, както на приходите, така и на разходите от международната миграция в измерения, като например: трудова миграция; обсъждане на въпроси, като миграция и развитие; интеграция на мигрантите; институционални мерки за управление на миграцията и съвсем не на последно място- взаимоотношенията между миграция и здраве" [4, 21].

3. Разработване на съвременни изследователски методики за проучване същността на миграцията. J. Salt и J. Hogarth отбелязват, че „разработването на тези методики е, все още, в своето ранно детство" [7]. Данните недвусмислено показват, че, често пъти, основни сведения се вземат от журналистически обзорни статии и коментарии, а не от добре замислени, структурирани и професионално проведени социологически проучвания, които да разкрият истинските и дълбоко скрити причини и същностни характеристики на миграционните процеси.

4. Търсене на нови и ефективни начини и средства за борба с незаконната миграция и трафика на хора, особено на деца и жени за сексуална експлоатация. Хр. Попов пише: „За съжаление, след повече от десетилетие на заострено внимание, изследванията върху трафика за сексуална експлоатация не са напреднали и отишли по-далече от картографирането на проблема и обзорите на правните рамки и административните отговори" [4, 10].

5. Намиране на най-сполучливи пътища и подходи за успешна социална адаптация и гражданска интеграция на мигрантите в приемащите страни, осъществявана заедно от държавните институции, неправителствените хуманитарни и религиозни организации.

6. Миграцията и изгнанието остават важна тема за науките в XXI век, когато хората продължават да бъдат насилствено преместени от войни или етнически прочиствания, или да мигрират повече или по-малко по свое собствено желание. Според Р. Кинг, „в свят, все още доминиран от нациите-държави и глобалните корпорации, миграцията създава социално приспособими и хибридни идентичности. Травмата, носталгията и отхвърлянето от обществото се балансират от плурализма, космополитизма и уважението към другите култури. Историята на миграцията никога няма да свърши, докато съществува човешката раса" [2, 13].

За да може да се обхване ролята на европейската политика в рамките на този процес, още повече пък за да бъдат очертани приоритетите му, са нужни позадълбочени анализи по тази тематика заради мащабите и сложността на насочените към Европа миграционни процеси. Миграцията е тема, която се числи към ос-

новните в ерата на глобализацията и това я прави предизвикателство, изискващо концептуални решения на всички нива- от стратегическо до локално. В този смисъл е малко вероятно ЕС да успее да постави всички аспекти на миграцията под контрол. По-реалистично би било, чрез умереното й контролиране, да се извлече максималната полза от нея, като се избегнат негативите и.

За да се справи с тази трудност, ЕС трябва да разработи дългосрочни планове, които да са съобразени с актуалните развития в страните-членки. Те обаче не са никак розови: повечето европейски страни са принудени да се борят с все по-драстични демографски спадове, въпреки че някои от тях са обект на трайни миграционни вълни. Очаква се, например, до 2060 година, населението на Германия да намалее от 82 на 65 милиона жители и то при запазване на сегашните миграционни темпове към страната. На една жена сега там се падат по 1,6 деца, при минимална стойност от 2,1 за поддържане на естествения прираст. Като сравнение могат да се приведат някои страни в Африка, които имат честота на удвояване на населението си под 30 години. През 2008 година в ЕС живеят 495 милиона души, като съотношението между работещи и пенсионери през тази година е 4 към 1. През 2060 година, обаче, се очаква то да падне до 2 към 1. Това поставя политиците пред изглеждаща невъзможна за решаване задача: как да се поддържа функционирането на държави, в които хората вече са на изчерпване. Само до 2020 година европейските икономики ще се нуждаят от допълнителни 16 милиона души квалифицирана работна ръка. Да, със сигурност, миграцията е основна част от решението. Но дали е единствената? Как да се обясни фактът, че се наблюдава масова безработица именно в държави със силни миграционни потоци, макар европейските страничленки да разчитат на мигранти в първичния (ИТ-експерти, лекари, медицински персонал, инженери) и вторичния (обслужващи професии- строителство, ресторантьорство, хотелиерство, транспорт, услуги, сервизи, които гражданите на „Стара Европа“ не искат да изпълняват) трудови сектори? Типичен пример за това е Кралство Испания- там в периода 2000 година-2005 година се наблюдава увеличаване броя на мигрантите със 194% (до 4,8 милиона) и то, въпреки проточилата се през цялото първо десетилетие на XX век и драматично задълбочила се след началото на финансовата криза икономическа рецесия, последствията от която са над 4 милиона безработни (младежката безработица достига дори 50%). За същия период в Италия броят на мигрантите е нараснал с 54%, достигайки 2,5 милиона. Бившият италиански външен министър Франко Фратини ще бъде запомнен с апела си за солидарно преразпределение на мигрантите между страните-членки, за да може страната му да си отдъхне от огромния поток мигранти от Африка- Либия, Еритрея, Сомалия, Судан, Египет. Обща тенденция в ЕС е бизнесът да призовава за разхлабване на регулациите, позволяващи на чужденци да се заселват на територията на Съюза, докато определени политически кръгове, както и обществеността, изразяват опасения за загуба на национална идентичност, културни завоевания и работни места. В тази връзка, логично възниква въпросът, дали общественото мнение в Европа, заето да претегля позитивните и негативните аспекти на миграцията, не бива съзнателно отклонявано от крещящата потребност за предприемането на решителни структурни реформи от европейските правителства?

II. Документи и институции, занимаващи се с въпросите за интеграция и адаптация на мигрантите

През 1999 година, Европейският съвет приема специален документ за бежанците и изгнаниците, наречен „Становище, относно интеграцията на бежанците в Европа” (10). Той е преработен и актуализиран, съобразно промените в политиката

на страните от Европейския съюз, по отношение на мигрантите през 2002 година. Този програмен документ лежи в основата на изработената обща европейска политика в областта на социалната адаптация и интеграция на бежанците.

Европейският съвет за бежанците и изгнаниците (ЕКРЕ) разглежда процеса на социална адаптация и гражданска интеграция като динамичен и двупосочен процес, който поставя редица изисквания, както пред приемащите страни, така и пред мигрантите [10]:

- По отношение на бежанците, се изисква готовност за приспособяване към начина на живот на приемащото ги общество, без да се налага загуба на културна идентичност.

- По отношение на приемащото общество, интеграцията е процес, който изисква желание за адаптиране на съществуващите обществени структури към настъпващите промени в облика на населението, приемане на бежанците, като част от националната общност и предприемане на действия за улесняване на достъпа им до ресурсите и механизмите на вземане на решения.

Позициите на мигрантите в процесите на социална адаптация и гражданска интеграция, според Презентацията на Агенцията за бежанците, са следните: „Интеграцията значи да се чувствам в новата страна като у дома. Интеграцията е като състезание по триатлон. Триатлонът на интеграцията включва:

- колоездене, т.е., да бъдеш в основната група;

- плуване, т.е., да си самостоятелен;

- тичане- почти си стигнал, но тук предизвикателството е най-голямо. Този, който продължи да тича е интегриран" [4] .

Към ООН съществува Бюро за международна статистика, което изучава миграцията в света. С цел осигуряване на най-добри условия за съпоставяне на националната информация и създаване на методологически основи за сравнимост, се поставят изисквания от ООН по отношение на данните, получавани от страните, съдържащи се в документите: Съвместен въпросник по статистика на международната миграция, с данни за Евростат, ООН, МОТ, Съвета на Европа; Регионален демографски въпросник на Евростат; Проект за Регулация на ЕС за статистика на международната миграция, гражданството, разрешенията за пребиваване и убежище. На тази основа се изграждат масиви за:

- Международните миграционни потоци- влизащи и излизащи от страните; дългосрочната емиграця и имиграция по гражданство, възраст и по последно местоживеене.

- Международна имиграция по пол, година на раждане и район на планирано заселване.

- Работещи и неработещи имигранти- по пол, възраст, образование, семейно положение, гражданство, статут и др.

В МОМ е в процес изграждането на джендър (gender)-статистика (включване на пола, като важен показател при събиране и извеждане на данни за международната миграция). Целта е отразяването на социалните явления и процеси, като се има предвид различната роля и отношение към тях на мъжете и жените и различния им принос за развитието на населението, икономиката и обществото, като цяло.

В последните две десетилетия избухват десетки войни и военни конфликти, създават се множество нови държави, появяват се милиони принудителни мигранти. От това назрява необходимостта от сериозен анализ на миграцията в социално-

педагогически аспект, за да се изведат общите тенденции и характерните особености на социалната адаптация и гражданска интеграция на всички видове мигранти.

Очевидно, миграцията е неоднозначен, дори поляризиращ и противоречив процес. Обвързаностите и участващите в него играчи покриват всички социални слоеве и групи по интереси, затова е необходим задълбочен подход при дефиницията на различните видове миграция. От гледната точка на интересите на ЕС (и долавящ се в стратегията му), най-резонно е мигрантите да се делят според квалификацията си на високо, средно и неквалифицирани, както и на легални и нелегални.

През 2007 година на територията на ЕС се намират 18,5 милиона души от т. н. „трети страни“. Това са 4% от цялото му население. В това число обаче не влизат онези, които вече са получили европейско гражданство. Трите най-многобройни мигрантски етноса в ЕС са турците (2,3 милиона), мароканците (1,7 милиона) и албанците (0,8 милиона). Общо, 9 милиона граждани на ЕС използват правото си на свобода на движение и пребивават в друга страна-членка. Броят на търсещите политическо убежище е спаднал до 200 000 души- своеобразно дъно, в сравнение с минали години. Миграционният баланс на ЕС за 2010 година е позитивен: заселилите се са с 1,75 милиона повече от напусналите (този метод, обаче, поставя на една и съща плоскост бежанци и студенти). Броят на нелегалните имигранти в ЕС се оценява на 4,5 милиона, макар вероятно да е значително по-голям. Към това се прибавя и фактът, че с приемането на държавите от бившия Източен блок в Съюза определени миграционни проблеми с ясно изразени социални измерения формално се прикриват от правото на свободно придвижване, но на практика продължават да са на дневен ред и дори се задълбочават. Актуален пример е разгорещеният през 2012 година спор около катуните на български и румънски роми във Франция, където европейската мобилност и номадският начин на живот се сблъскват по впечатляващ начин и истерията във Великобритания през 2013 година от Найджъл Фараж и неговите поддръжници от Партията на независимостта по отношение на българските и румънски граждани, получили право от 01. 01. 2014 година свободно да се придвижват и работят в целия ЕС.

Миграционните процеси поставят милиони деца, младежи и възрастни в необичайна ситуация- те се сблъскват с нова култура и език, специфична образователна система, други възпитателни модели, различни нравствени и естетически ценности, особени социализиращи фактори, нова, често пъти, коренно различна социална психика и социално поведение на обществото и личността. Това извежда потенциалните ученици и студенти пред трудно преодолими противоречия, свързани със светоглед, религиозни вярвания, отношения към семейството, жената и децата, модели на поведение, мотивация за учене и труд.

Що се отнася до легалната имиграция, на политическо ниво, в Европа може да се говори за едно позитивно отношение, водещо и до редица конкретни инициативи. Приемат се закони, които разрешават на имигрантите, след работен престой от минимум една година, да се съберат със семействата си. Лица, които от пет години легално пребивават на територията на ЕС, могат да получат разрешение за дълготраен престой, което им дава възможност да преминат на по-високо ниво на квалификация или пък да работят в друга държава-членка на Съюза. Други нормативни актове касаят въвеждането на общоевропейски приемни критерии за студенти и научни работници. Особено внимание заслужава инициативата за т. н. „синя карта“, която представлява ускорена процедура за допускане до работния пазар на конкретна страна-членка на висококвалифицирани професионалисти при особено благоприятни условия на престой, включително предоставяне разрешение за рабо-

та в целия ЕС след период от две години. Във все по-взаимосвързания глобализиран свят се лансират нови концепции като алтернатива на досегашните миграционни явления. Сред тях си заслужава да бъдат споменати „циркулиращата миграция“ (престой на чуждестранна работна ръка за определено време, след това завръщане в родната страна и приложение на придобитите компетенции и знания там), концепцията за „социалните преводи“ [1] (пренасяне на западни ценности и работна култура в родната страна на мигрантите), и „мозъчна циркулация“, вместо традиционното „изтичане на мозъци“. Взема се предвид и опцията, с оглед на интеграционния процес, да се взаимодейства по-тясно с изградените в приемащите държави имигрантски мрежи, доскоро смятани за опасни и формиращи паралелни културни общества.

От друга страна, ЕС си е поставил като приоритетна задача да противодейства на нелегалната имиграция. Всяка година 500 000 нелегални имигранти биват арестувани на европейска територия; от тях средно 40% са върнати обратно в родните им страни, още 300 000 пък биват спирани още на границата. На този приоритет се придава допълнителна значение и поради факта, че нелегалната имиграция и международната организирана престъпност си взаимодействат, което пряко засяга европейската сигурност. ЕС преследва тази цел с вътрешни (строги санкции срещу работодатели, назначаващи нелегални имигранти, като някои държави-членки се задължават да засилят трудовия си контрол) и външни мерки. Инструментите, с които разполага Съюзът са Европейския фонд за външни граници, Европейския фонд за връщане и Европейската агенция за управление на оперативното сътрудничество в периферните региони или накратко Фронтекс. Последният се занимава с провеждането на общи операции (към настоящия момент 25 на брой) по сухопътните и морски граници, както и на летищата на ЕС с цел да се попречи на нелегалните имигранти да достигнат европейската територия.

Миграцията обхваща огромни човешки маси от различни националности, вероизповедание, светоглед, цвят на кожата, възраст- от новородени до хора от третата възраст, които желаят на всяка цена да завършат земния си път в своята Родина и родно място. В този аспект, проблемите на миграцията засягат всички отрасли на науката и се поддават на разбиране само чрез комплексни възгледи, оценка и проучване.

Миграцията оказва изключително силно въздействие и върху нравственоетичното състояние на гражданите на приемащата държава. От една страна, част от населението осъзнава човешкото страдание и е готово да разделя с имигрантите част от националното богатство, а от друга страна, налице е силно изразен негативизъм към чуждоезичните, към техните традиции, религиозни вярвания и обичаи. Мнозина мигранти, според R. King, „страдат от липса на квалификация, от унижението, расизма и разрушаване на здравето им...Глобалното разделение на труда е внедрено от капиталистическите сили, които поощряват неравенството и отричат възможността за достоен живот за всички, включително за многото имигранти” [(2, 13].

- Миграцията винаги е била, а сега, през XXI век е особено ярък елемент на общите глобализационни процеси в света. Тя носи със себе си два ясно изразени белега- позитивно влияние и негативно отношение, от страна на националната идентичност и култура. Миграцията, според R. King, е „тройно печелившо” положение, от което се възползват еднакво и изпращащите, и приемащите страни, както и самите преселници. Това тройно печелившо положение е осъществимо, при условие, че миграционният процес е добре управляван и са взети необходимите мерки, за да гарантират достойнството, човешките права и благоденствието на

имигрантите. Твърде често са налице негативни последствия и съвременният свят продължава да е негостоприемен към преселниците" [2, 13].

Създаването на законодателна база, свързана с въпросите на мигрантите, бежанците, националните малцинства, съотечествениците зад граница, изисква приемане на редица положения, инструкции, както за всички проблеми, така и за отделните категории лица и за отделните сектори на социалната дейност- социална адаптация и гражданска интеграция (получаване на образование, включително и висше, събиране на семействата, придобиване на професия и бъдеща реализация в трудовата дейност, постоянно местоживеене, приобщаване към културните ценности и традиции на приемащата страна и др.).

Интеграционната политика на ЕС, днес, е насочена към това, щото „мигрантите да запазят своята идентичност и други културни характеристики (език, религия, музика, хранителни навици, празници, дрехи и др.). Макар и подкрепено официално, поддържането на културната идентичност, съчетано с неравенство в правата, продължава да бъде извор на конфликти и дискриминация" [5, 19].

За много бежанци и принудително преселени лица, правните и социални гаранции в различните страни и по различни причини не могат да бъдат съблюдавани на ниво общоприети стандарти, което, от своя страна, предизвиква сериозно безпокойство в Управлението на Върховния комисар по въпросите на бежанците на ООН, а, също така, и в други хуманитарни обществени организации.

Заключение

Масовата миграция води до изменение на структурата на населението, укрепва местните национални диаспори в съответните страни и по-специално в Англия (индийска, пакистанска, афганска, иракска, иранска, руска, полска, българска, африканска- групиране на хора от различни африкански племена и държави, арабска и др.), което, от своя страна, създава допълнителни предпоставки за възникване на конфликтни ситуации на битова или международна основа.

От тази гледна точка, днес, в условията на глобална финансова, икономическа и производствена криза, Обединеното кралство се оказва в твърде деликатна ситуация- от една страна, подписани и ратифицирани са всички международни актове, адаптирано е законодателството в областта на имиграцията с международните изисквания, а от друга страна, не може да оказва цялостна и качествена помощ на преселниците, поради намаляване на средствата за тази дейност, растящата безработица сред собствените й граждани и нарастващото социално напрежение.

Съвсем справедливо звучат думите на държавните ръководители от най-развитите страни за по-силното и действено включване в тази дейност на църквата, неправителствените организации, доброволните сдружения, комитетите, които разполагат с подготвени хора и сравнително добри материални и финансови ресурси и средства.

Литература

1. Европейска комисия, Генерална дирекциа „Изследвания и иновации" (2012): State of the Innovation Union 2011. Служба за публикации на Европейския съюз, Люксембург.

2. История на човешките миграции, Под общата редакция на Р. Кинг, CIELA, С., 2009.

3. Попов, Хр., Трафик на жени. Причини, последствия и противодействия, ИК „ЛИК", С., 2007.
4. Презентация на Агенцията за бежанци, Айдахо (САЩ)-София (България), С., 2003.
5. Сачкова, Е., Развитие на интеркултурната педагогика в Европа (по материали на Съвета на Европа), Педагогика, кн. 4, 1997.
6. Boswell, Christina & Andrew Geddes, Migration and Mobility in the European Union, Palgrave Macmillan", London, UK, 2011.
7. Salt, J., J, Hogarth, Trafficking and human smuggling in Europe: A review of the evidence, Geneva, International Organization for Migration, 2000.
8. The Economic and Social Impacts of Immigration, Minister of Supply and Services, Ottawa, ON, 1991.
9. UNHCR, Global Appeal 2012-13, The UN Refugee Agency, New York, 2013.
10. http//www.ecre.org. Становище на ЕКРЕ, относно интеграцията на бежанците в Европа.

ДОБРИ ПРАКТИКИ НА АНГЛИЯ В ОБЛАСТТА НА МИГРАЦИОННАТА ПОЛИТИКА И ВЪЗМОЖНОСТИТЕ ЗА ПРИЛОЖЕНИЕТО ИМ В БЪЛГАРИЯ

Чавдар Л. Милков

EFFECTIVE PRACTICES, FORMING THE BASIS FOR THE UK POLITICS AND POLICES AROUND MIGRATION AND THE OPPORTUNITY OF IMPLEMENTING THOSE IN BULGARIA

Chavdar L. Milkov

ABSTRACT: *Authorities in the UK acknowledge and accept that the social adaptation and the integration of migrants in the UK is a complex and lengthy process. It is a process filled with with many obstacles that need to be overcome. These obstacles are from a various nature - political, educational, social, religious, financial, cultural, moral. The progress achieved in the UK can be analysed and interpreted by the Bulgarian government in order to successfully complete the task of integrating migrants in the country.*

KEY WORDS: *Migration, integration in the society, social adaptation, positive examples, system for integration.*

Увод

Социалната адаптация и гражданската интеграция на кандидатстващите за убежище започва от момента, в който те пристигнат в общината и се поемат от системата „Социално подпомагане", или от имиграционните власти. Изключително важно е, този процес да не бъде отлаган за по-късен период, защото това води до допълнителни трудности от здравословен, социален и юридически аспект.

Основна задача на социалните работници и първи стъпки в процесите на социализация и интеграция, са в сферата на намиране на подходящи (съобразно възрастта, националността, етноса, религиозните убеждения и други фактори от практическо естество) места за живеене. Цели се, не само осигуряване на практически годни условия за живеене, а и предоставяне на подходяща семейна среда, като приемни семейства или детски домове. Пристигащите деца са с ограничени способности да се грижат за себе си без чужда помощ, с минимални или нулеви познания за език, култура, общуване, социална среда, традиции, закони, нрави, обичаи в приемащата страна. Те нямат родители, приятели, в повечето случаи, никаква връзка с хора от същата държава, етнос и религия. Приемните родители са тези, които осигуряват изключително необходимата психична стабилност и практически грижи в този начален адаптационен период.

Друг аспект от стъпките при социализацията и интеграцията в този ранен период е осъществяването на връзка с юридически лица (по-специално, адвокати) и посредством тях, по-нататъшна връзка с имиграционните власти. Директните контакти на детето с адвокатите и имиграционните власти са времево ограничени, необходимо е те да се срещнат в рамките на един месец, за изясняване на причините, довели до търсенето на убежище.

За да улеснят и подпомогнат процеса на цялостната интеграция и социализация на новодошлите, социалните работници провеждат странично и обстойно изследване. То е насочено към здравословното състояние на детето, нивото на образованост, религиозните и практически потребности- вид храна и режим на хранене, необходими диети, рутина на живот, сън, чувства; комуникативни умения и способности; семейна история; история на междуличностните отношения в семейството и установяване на позициите на детето в него- равнопоставеност, педоценризъм, осъществявано насилие или безразличие от страна на възрастните към него.

Изследват се ролята и задълженията на децата в семействата им, участието им в различни видове труд, предполагаемо или евентуално участие във вътрешни въоръжени или военни конфликти. Проучват се степените на социална зрелост на децата; участието им в религиозни, социални или политически детски и младежки организации; наличието на верски фанатизъм; битов консерватизъм; нивото на сексуална култура и сексуалност; отношението към жената и майката, към семейството; вероятното участие в т. н. уредени бракове (за ислямските държави) .

I. Форми на дейност на системата „Социално подпомагане“ в община „Търък“, Есекс, Англия

Благодарение на изследването на гореспоменатите области, социалните работници от общинска служба „Социални грижи” определят степента на цялостно развитие и зрелост на детето. В резултат на това, се формулира и изработва план за по-нататъшна адекватна подкрепа за детето.

В отделите на системата „Социални грижи” към общините се изработват планове за грижите, необходими за всяко дете, като се прави възходяща градация на тях, по степен на значимост, тъй като всяко дете е с различна степен на зрелост и потребности. Въз основа на тези планове, социалните работници съдействат за връзката на децата с учебните заведения в общината, местата за изповядване на религия (в община „Търък” има действаща джамия за изповядващите исляма и няколко църкви за различните направления в християнството, но липсват будистки храмове), здравните власти (личен лекар, поликлиники, болници).

Системата „Социални грижи” поема и финансовата издръжка на децата, кандидатствали за убежище, включваща: седмична парична издръжка; осигуряване на транспортни разходи; средства за образование (общината заплаща пълната такса за обучение, стойността на всички учебни помагала и пособия, дава допълнителен седмичен паричен стимул на онези деца, които се обучават в колежански форми); средства за облекло, обувки.

Миграцията е двуполюсен процес, от една страна, се очаква имигранта да положи усилия, да се адаптира и приобщи към новата образователна, културна, социална среда, а от друга страна, той допринася за обогатяването на многообразието на същата тази среда. По тази причина, общинските социални работници се стремят да стимулират у тези деца желанието да запазят и съхранят своите нравствени, културни, семейни ценности.

В община „Търък” това се осъществява посредством създадените групи от кандидат-бежанци, в които се провеждат културни, спортни, религиозни, социални занимания и където им се предоставя възможност да се срещат с представители на своя етнос и народ.

Социалните работници от общината се грижат и за осъществяването на връзки между търсещите убежище деца и много неправителствени организации- Британски червен кръст и др. Те помагат при осъществяването на контакти със страната, родителите, близките и роднините на децата. Други НПО работят в сферата на оказване на помощ на лица с ментални заболявания: „Британска медицинска фондация”- „British Medical Foundation” и фондацията „Хелън Бамба”- „Helen Bamber Foundation”.

Осигурени са необходимите връзки в процеса на свързване на децата-мигранти с различни терапевти от организацията „Отворени врати”- „Open Door”.

Друг, който подпомага изключително активно и резулттатно адаптацията, социализацията и интеграцията на децата-мигранти в община „Търък“ е организацията „Връзки”- „Connexions”. Тя е създадена по инициатива на правителството и действа на национално ниво. Предлага съвети и насоки за деца и млади хора, между 13 и 19 години, по отношение на: обучение и образование в средни училища, колежи и университети; места за живеене; работа; финанси; квалификация; алтернативни форми за придобиване на образование и специалности; професионално ориентиране; здравно и психо-соматично здраве; умения за общуване, контакти и взаимоотношения с различни видове хора- по пол, възраст, образование, религиозни вярвания, етноси, раси; информация за услуги и институции в общината.

В центровете на тази организация децата могат да получат и някои документи за идентификация.

За лицата, които са без образование, общината осигурява постъпване в задължителни езикови курсове по английски език, с продължителност минимум 6 месеца. След частично овладяване на езика, макар и на ниско ниво, децата се настаняват в училища, където с тях се работи индивидуално по няколко програми за социална адаптация и гражданска интеграция- допълнителни часове по английски език, английска културна история, история на света, човекът като личност. Запознават се с традициите, нравите и обичаите на съвременното английско общество. Участват във всички училищни и извънучилищни мероприятия- празници, ритуали, екскурзии, активен отдих. По този начин се създават условия за засилени контакти между децата-имигранти и местните деца, за постигане на равнопоставеност и толерант-

ност в отношенията. Налице е висока религиозна толерантност и се избягват проблемите, свързани с изповядваната религия. В общината се полагат сериозни усилия за съхраняване на културната и нравствена идентичност на имигрантите.

Другата група имигранти- тези с образователна степен и грамотност, също посещават интензивни курсове по английски език. По-късно те се записват в различни класове, в зависимост от образователната степен и ниво на владеене на английски език. Социалната адаптация и гражданската им интеграция протича по различен начин. За част от изследваните лица установихме, че този процес протича по-бързо и динамично. Децата и младежите желаят да се интегрират в английското общество, да получат образование, усвоят професия и се реализират на пазара на труда.

Част от тях имат сериозни проблеми при интеграцята и адаптацията- срещат съпротива от страна на консервативни родители, силно вярващи, които не разрешават на момичетата и жените да ходят в смесени училища, да усвояват бързо английски език. Тези лица, по-късно имат сериозни проблеми с приобщаването към ценностите на английстото общество- не владеят езика, носят традиционното за жените и мъжете ислямско облекло, нямат професия и образование. Те непрекъснато са на социална издръжка и помощи, което затруднява общинския бюджет.

Като изхождаме от опита на развитите западноевропейски държави, САЩ и Канада, от политиката на правителството на ОК и от собствения си опит в общинската дейност (теоретически и практико-приложен), свързана с мигранти, в продължение на близо десетилетие, както и от резултатите, получени от изследването, можем да изведем следните водещи принципи, задължителни при реализацията на социалната адаптация и гражданска интеграция на принудителните мигранти в ОК:

- Необходимо, е според нас, при решаване на проблемите им да се подхожда от презумпцията, че голяма част от тях ще останат постоянно или за продължително време в ОК, конкретно в общината. Те могат да допринесат с труда и дейността си за просперитета на страната в икономически, културен и социален аспект.

- Да се осъзнае решаващата роля на държавните и общински органи в процесите на адаптация на имигрантите и в развитието на добри отношения между тях и населението. Това, от своя страна, дава основание за изискване от органите на местно самоуправление на законодателна база за мерките, които ще осигурят постигане на равни възможности, отхвърляне на дискриминацията и създаване на условия за тяхната безпроблемна интеграция и социализация в британското общество. От друга страна, необходимо е да се поощрява в чужденците чувство за принадлежност към новото общество. Властовите структури и обществените организации е добре да приемат имигрантите и техните лидери като партньори за установяване на междуетнически, междурасови и междукултурни отношения.

- Трябва да се разбере, че интеграцията, социализацията и установяването на добри отношения с местното население е процес, разчетен на дълги периоди. Международните конвенции и опитът на редица страни потвърждава, че имигрантите, живели продължително в приемащата страна, особено онези, които са се родили в нея, трябва да имат възможност без пречки и трудности да получават гражданство, което е най-ефективния способ за развитие у тях на чувство на принадлежност към обществото, в което живеят и работят.

- Значително подобряване на положението на чужденците може да настъпи и при активизиране на техния собствен социален потенциал. ОК, и по-конкретно, Англия, поощрява създаването и функционирането на асоциации на мигрантите и

етническите групи, на която база се създават обществени фондове, предназначени за разработка и реализация на проекти, отразяващи интересите им. Първостепенно значение се отдава на религията, културата, традициите, обичаите, празниците, с цел уважаване правата на човека. Позитивни резултати добиват онези органи на властта, които се стремят да установят контакт с представителите на различните конфесии и организират обсъждане на проблемите им, в съответствие на интересите, както на местното население, така и на придошлите чужденци.

Нерядко местните органи на самоуправление предоставят на чуждестранните общности възможност за участие в културния живот на местното население. Важна роля играят онези масмедии, които поощряват всякаква дейност, насочена към това, щото местното население да проявява лоялност и търпимост при взаимоотношенията си с новопристигналите. Технологията на социалната работа с мигрантите може да донесе позитивни резултати при наличието на гъвкава и обмислена политика и програма за прогнозиране на миграционните процеси и конкретните миграционни потоци (по пол, възраст, религия, образование, етническа принадлежност, народност и др. показатели), регионални имигрантски програми, съдействие на чужденците в процесите на адаптация към новите места на живеене.

В съвременните публикации, изказвания и позиции на лидери на различни политически партии, сдружения, НПО, се констатира колизия, която трябва да се разреши по някакъв начин. От една страна- рязка реакция на някои обществени слоеве, партии и публични личности към имиграционните потоци, заливащи ОК, а от друга- невъзможността да се възпрепятства имиграцията и потребността на същите тези слоеве от имигранти. Пред лицето на тази колизия Обединеното кралство не е единно- съществуват диаметрално противоположни позиции, възгледи, мнения и политики, засягащи миграцията. Удовлетворителни решения, поне засега, не са намерени, въпреки продължителния опит в областта на имиграцията и съответстващата й имиграционна политика.

В тези условия е необходимо интензивно търсене на оптимални подходи при избора на имиграционна стратегия. Преди всичко, важно е да се разбере страха на обществото в сегашната икономическа, финансова и банкова криза от нарастващия приток на хора от други националности, доколко той е обективно обусловен и какви мерки са необходими за туширане на нарастващото напрежение. В каква степен този страх се продуцира от битуващите в обществото стереотипи, раздухвани от користни политически или други интереси, и в такъв случай, как обществото може да преодолее този страх.

В тази дейност е важна ролята на експертното съобщество- научни работници, журналисти-аналитици и специалисти-практици. Развитието на дискусията вътре в това съобщество и постоянният диалог с политиците и най-широките обществени слоеве на населението са едни от най-важните пътища за решаване на сложните обществени проблеми, към които, безусловно, се отнася и формирането на такава имиграционна политика, осигуряваща баланс на интересите, стабилност и безопасност в страната.

II. Изводи за практиката на системата „Социални грижи“ в Република България

В резултат на обсъждането на имиграционните проблеми, по отделни, ключови въпроси, достигаме до следните заключения, които с известна адаптация могат да се реализират в Република България:

1. ОК изпитва потребност от мигранти. В последните години и по прогнози за бъдещето се наблюдава сериозно застаряване на населението. В редица райони на кралството плътността на населението не отговаря на икономическите потребности- работна сила в селското стопанство, в преработвателната индустрия, в промишлеността. Там е налице дефицит на трудови резерви.

2. Неизбежният ръст на имиграцията в ОК е свързан не само с това, което се случва в страната, но, на първо място, с това, което се случва в света- войни, природни колизии, екопроблеми, бежанци, преселници, мигранти, расови и етнически сблъсъци и прочиствания.

3. Притокът на мигранти от други култури и религии носи сериозна заплаха. ОК трябва да е готово да приеме това предизвикателство- искания за построяване на джамии, обредни домове, културни центрове, производство на специфични храни (например, без свинско месо за мюсюлманите) и др. Тази готовност трябва да се изгражда сега, в настоящия момент, но за съжаление, британското и световно интелектуално съобщество, досега, не са намерили удовлетворителен отговор на тези предизвикателства.

В Република България въпросът с култовите и обредни домове на изповядващите исляма не стои така остро, както в Западна Европа, тъй като е налице национална система (Главно и областни мюфтийства, множество джамии, подготвени религиозни лица- имами, ходжи, специалисти по изучаване на исляма).

4. Много от обсъжданите проблеми не са специфични за имиграционната политика. Това са общи проблеми на изграждането и запазването на гражданското общество и институтите за формиране на политика във всички области на развиващия се социум.

5. Един от концептуалните проблеми в политиката по отношение на инокултурната, разноезична и религиозна имиграция е противоречието между либералния подход, опиращ се на гражданската идентичност и наличието на бързо нарастващото етническо самосъзнание. Слабостта на либерализма се крие в това, че игнорирайки етническото, той отказва на имигрантите идентичност, която изостря противопоставянето на различните етноси в обществото.

6. Политиката към различните етнически имигранти и ситуацията, в която те се намират, има различни нюанси в отделните части на ОК- по-крайна е в Северна Ирландия, където има голяма безработица, нравствена, социална и гражданска разруха, религиозно напрежение между католици и протестанти, ИРА, все още, е много активна и проповядва ненавист към всички чужденци, включително и към англичаните, а в Англия политиката към имигрантите е по-приемлива- търпимост, етническа и религиозна толерантност.

7. Един от позитивните резултати на чуждоетническия приток в ОК е възникването на поликултурна среда за децата- расте поколение с друга, по-динамична установка, нагласи, възприемане на другия, готовност за съвместен живот в обществото, училището, университета и работното място, с представители на други раси, религии, етноси, култури, езици. Това е вариант на еволюционно формиране на мултикултурна идеология.

8. Имигрантите не представляват за населението на ОК конкуренция на пазара на труда. В Република България настоящите и бъдещи имигранти ще се влеят, чрез пазара на труда, в индустрията, търговията, селското стопанство, леката промишленост и всички други области на стопанската дейност, ще създават материални и

духовни блага. Чрез приемането на мигранти могат да бъдат решени множество сериозни проблеми- обезлюдяването на редица райони и региони в страната (села, малки градове, Северозападния район) може да бъде преодоляно чрез заселване на мигранти.

9. Криминогенните прояви на имигрантите заемат неголяма част от общия брой престъпления и не надвишават значимо криминалните действия на коренното население.

Авторът защитава позицията, че миграционната политика е съвкупност от социално-политически концепции и възгледи за международната миграция, организационно-правни и социално-икономически мероприятия, насочени към регулиране на миграционните процеси, както във всяка отделна страна, така и във всеки район, регион, окръг, община. Миграционната политика на развитите страни, включително и на ОК, е неотменна част от международните отношения и вътрешната политика.

Заключение

Засилената днес миграция е ярко изразен аспект на всеобщите глобализационни процеси, обхванали целия свят- континенти, държави, капитали, идеи, движение на огромни човешки маси, ноу-хау. Неразрешената миграция се проявява тогава, когато имигрантите нарушават определения във визите им срок за престой в приемащата държава или работят без задължителните пред законите разрешителни. Някои имигранти просто изчезват след отхвърлянето на молбата им за убежище, други се промъкват през границите с фалшиви документи или не се регистрират, когато това се изисква от закона. Въпреки наличието на все по-строг имиграционен контрол, един значим компонент от миграцията се състои от хора, които отиват или пребивават в чужди държави незаконно.

Проблемите на миграцията и търсенето на убежище са преплетени с правата на човека, тяхното зачитане и спазване в съвременния свят.

Изследванията на правителствени и неправителствени организации, фондации, асоциации, сдружения показват, че в основата на миграцията на хората стоят множество значими проблеми от различно естество: икономически (липса на възможности за реализация на пазара на труда, ниско заплащане, мизерия, нищета, бедност и др.), военни (конфликти, войни, граждански вълнения, подтисничество), религиозни преследвания, политически промени, водещи до гонения, нарушаване на човешките права и свободи, екологични катастрофи.

Специфичните особености на миграцията през XXI век са обусловени от това, че в условията на изострени социални, културно-цивилизационни проблеми, войни и конфликти, разпад на многонационалните държави (Югославия, СССР, Чехословакия) и образуване на нови, независими страни, на преден план излизат въпроси, свързани с доброволната и принудителна миграция (бежанци, екологични мигранти, етнически и религиозни прочиствания).

ЛИТЕРАТУРА

1. Абросимов, Св., Кризата: новото преселение на народите, Сега, 04. 04. 2009.

2. Европейска стратегия и политика за интеграция на мигранти, ЕС, Брюксел, С, 2012.

3. История на човешките миграции, Под общата редакция на Р. Кинг, CIELA, С., 2009.

4. Национална стратегия за миграция и интеграция 2008-2015 година, С., 2008.
5. Brubaks, T., W. Comment, Controlling Immigration: A Global Perspective, W. A. Cornelius, P. L. Martin, J. F. Hollifield (eds.), Stanford, Stanford University Press, 1994.
6. Children and Young Persons Act, 2008, Parlament of Great Britain, London, 2008.
7. Department for Communities and Local Government, Managing the Impacts of Migration: A Cross-Government Approach, London, 2009.
8. Poppleton, S., L. Rice, The organization of asylum and migration policies in the UK, UK border Agency, London, 2010.

ВАИМООТНОШЕНИЯТА „ДЪРЖАВА-ГРАЖДАНСКО ОБЩЕСТВО“

Чавдар Л. Милков

Община „Търък“, Англия, Дирекция „Социално подпомагане“

THE RELATIONSHIP „STATE-CIVIL SOCIETY“

Chavdar L. Milkov

ABSTRACT: *In a democratic state it is expected of the civil society to rise and take steps to protect its people from the waywardness of the authorities in cases when the rights of the electorate are violated. We often observe a passive civil society in Bulgaria. This creates a feeling that it exists only formally.*

KEY WORDS*: Democracy, civil society, state,citizens activity.*

Въведение

Според текстовете на Конституцията на Република България, цялата власт в страната произтича от народа. Народът делегира тази власт на избрани, за да осъществяват управлението на държавата от негово име. Такива са принципът на демократичното управление и механизмът на функциониране на демокрацията във всяка страна по света, където е приет този модел на държавно управление. У нас, обаче, все повече нараства недоверието и недоволството на гражданите от управляващите и от работата на държавните институции. Народът, който по право е източник на властта, е все по-често пренебрегван в името на частните или партийни интереси на управляващите. Първия индикатор, който насочва вниманието към това заключение е намаляващата избирателна активност при провежданите в последните години демократични избори. Самият акт на гласуване, по същество, е упълномощаването на народни представители да осъществяват властта, която правото и законите поверяват на всеки един гражданин. В България хората са обезверени и рязко и драстично спада доверието в държавата. Примерите, които виждаме от Европа и по света, ни показват, че реално, демокрацията предполага, когато държавата в лицето на онези, които упражняват публичната власт, погазва и нарушава правата на своите избиратели, гражданското общество да се активизира

и да предприеме необходимото, за да защити хората от всякакви своеволия. В България наблюдаваме в повечето случаи едно пасивно гражданско общество, което създава усещането за формалното му съществуване. У нас, по-скоро, сме свидетели на една пасивност от страна на държавата, която в цялата досегашна демократична история, не е провела нито един референдум за допитване до своите граждани по важни, нашумели и наболели обществени въпроси. Изборите, които са основен демократичен акт, се опорочават все повече. В политическото пространство в последните години се срещат едни и същи лица, които „преяждат“ с власт. Държавата бива ограбвана ежедневно по всякакви начини и, за съжаление, очите на хората и на гражданското общество остават затворени за много беззакония.

Подобна незаинтересованост може да доведе до изключително неблагоприятни последствия, които ще засегнат, най-вече, социума във всичките му измерения-семейство, брак, отглеждане и възпитание на децата, формални и неформални групи, безработица, социална и материална нестраведливост, криза на моралните ценности.

В цялото това криво разбрано демократично поведение започва да настъпва политически и обществен хаос. Към настоящия момент политическите партии в България са над 170. Това е брой, редуциран по искане на прокуратурата от над 370 политически формации. Регистрираните неправителствени организации са между 23 000 и 25 000, като реално действащи от тях са не повече от 5000. Популярно в последните години стана формирането на граждански сдружения, които прерастват в партии и всячески се стремят, не към реализация на гражданското им предназначение, а към реалната политическа власт.

Във всяка сфера на обществения живот витае едно усещане за безнаказаност, за пълно неспазване на законите, от страна на упражняващите власт. Интересното е, че това не засилва влиянието и активността на гражданското общество. То остава, често пъти, като незаинтересован наблюдател на случващото се.

За създаването на политическа партия са необходими голямо количество средства и ресурси, т. е, въпреки твърдението на Конституцията, че всички са равни и имат идентични права, всъщност до политиката и до управлението на държавата имат достъп само тези, които имат финансова и икономическа възможност. От това следва, че в управлението на държавата присъстват само онези, които имат финансови ресурси. Предполага се, че това са между 10 и 20% от обществото. Изводът е, че властта притежава само тази част от гражданите, които имат възможности, а останалите между 80 и 90% са негласно дискриминирани. Това води до естествени и логични конфликти в общество, сред които най-наболял е съвременният социален конфликт. Все повече се налага необходимостта от силно, стабилно и активно гражданско общество. Негова основна функция и задача трябва да бъде да постига едно здравословно равновесие между държавата и обществото и да играе ролята на регулатор на отношенията между управляващи и управлявани. Гражданското общество е този балансьор, който трябва да следи и да отговаря за опазването и защитата на правата на отделните индивиди.

В противен случаи ставаме свидетели на нещо, което може застрашително да задълбочи. Лицата и партиите, които се наблюдават в последните години в българското политическо пространство се повтарят непрестанно. В един момент се получава следното: когато една партия е в опозиция критикува действията на управляващите и предлага редица решения за всеки възникнал въпрос. Когато премине в

управлението започва да установява, че няма ресурси, че едно или друго решение е неконструктивно. И така, години наред сме свидетели на липса на политическа ангажираност по важни обществени и социални въпроси.

Формирането на гражданското общество е естествения и логичен резултат на демократичната система. Разбирането за гражданското общество в нашето съвремие е общество, което е самоинициативно и активно. Съществуването на активно гражданско общество е един от начините да се преодолее развиващата се псевдодемокрация и усещането на огромната част от гражданите за безизходица от проблеми от изключително важно значение- корупцията в съдебната система и МВР, болезнените въпроси в областта на здравеопазването и образованието, престъпността. Политическият модел, който е установен в нашата страна, не е ефективен вече, тъй като голямата част от населението остава неудовлетворено и с усещане за погазване на основни човешки права и свободи.

Гражданското общество е длъжно в такава патова ситуация, да прояви своята роля на морален коректив и да заеме своята активна гражданска позиция. Все пак, гражданското общество е съставено от групирали се помежду си хора, чийто права са накърнени по някакъв начин, или са обединени от някаква обща инициатива, т. е., всеки сам за себе си е най заинтересован от следенето на собствените си права. Наличието на силно и самостоятелно гражданско общество означава това, че когато за който и да е гражданин настъпи ситуация, в която държавата не е реагирала адекватно или е проявила бездействие, да намери онази организация, гражданско обединение, където ще намери защита на своите интереси.

I. Концепции за граждански контрол

Един от преките изрази на демокрацията е контролът на гражданите върху дейността на администрацията. Осъществяването му е от изключително значение за нормалното протичане на демократичното управление и за гарантиране спазването на човешките права. Прилагането на гражданския контрол води до положителни резултати и за двете страни в процеса. От една страна, гражданите имат гаранция за опазване на своите права, а, от друга, администрацията получава обратна връзка за своята дейност и за предоставяните публични блага и се стреми към усъвършенстването си.

Съществуват редица концепции за прилагането на гражданския контрол. В последните години в България след поставяне на демократичното начало у нас, понятието „граждански контрол“ придобива съвсем нов смисъл. Прилагането на контрол от страна на гражданите е непознато и постепенно навлиза в разбирането на хората за управление, в което всеки гражданин може да изкаже своето мнение. До този момент формите на граждански контрол прилагани в развитите европейски държави и редица страни по света, не могат да бъдат адекватно въведени.

Гражданския контрол като понятие и прилагане се заражда в края на XVIII и началото на XIX век. Основните концепции са за: професионализма; делегирания и активния граждански контрол; интервенцията; споделената отговорност; съгласието; толерантността.

Автор на концепцията за професионализма е С. Хантингтън- САЩ, известен с парадигмата за „сблъсъка на цивилизацията“. Неговата теория се основава на професионализма в държавната служба. Той извежда два модела за граждански контрол- субективен и обективен. При субективния граждански контрол отношенията между държавата и гражданите се разглежда като система, в която нито един от

елементите не може да бъде променен без да доведе до промяна в останалите. Основните елементи в тази система са ролята на държавните органи, влиянието им върху обществото и принципите и идеологията, които изповядват. Необходимостта от граждански контрол произлиза от изискването действията на администрацията да се обуславят от законово определени цели, които да са в полза на обществото.

Обективният граждански контрол дава възможност да се определи в каква степен контролът от страна на гражданите оказва влияние върху институциите.

Концепцията за делегирания и активния граждански контрол е на социолога М. Яновиц. Той разглежда делегирания граждански контрол като възможност гражданите да участват и да се намесват в управлението по въпроси от обществено значение. Активния граждански контрол, според М. Яновиц, се определя като прекалена обвързаност на гражданите с политическата власт. Като социолог авторът използва методи, чрез които да установи по какъв начин развитието на гражданското общество оказва влияние върху дейността на публичната власт. Концепцията за делегирания и активния контрол е модел за взаимовръзката между държавата и гражданското общество.

Автор на концепцията за интервенция е С. Файнър. Той смята, че гражданският контрол е резонанс на характера и темперамента на обществото. С. Файнър твърди, че равнището на намеса на гражданското общество зависи пряко от неговата политическа култура.

Сред авторския колектив на концепцията за споделената отговорност е и Д. Бланд- канадски изследовател на въпросите за сигурността. Той смята, че проблемът при прилагането на граждански контрол възниква тогава, когато управляващите органи и политиците, поради некомпетентност или други причини не изпълняват своите задължения и отговорности. Основата на концепцията за споделената отговорност е идеята за консенсус между отделните страни. Авторите определят споделената отговорност като основен принцип във взаимоотношенията между гражданското общество и властта, в общества, където се наблюдава активно изразяване на гражданска позиция и гражданска инициатива по значими въпроси.

Автор на теорията на съгласието е Р. Шиф. Тя разглежда гражданския контрол чрез неговите съставни елементи- държавни институции, политическа система и граждани. Основната цел на тази теория е да се покаже необходимостта от провеждането на адекватен социален диалог. В своята теория Р. Шиф разглежда културния аспект и ценностите на обществото като основен фактор за реализирането на този диалог. Същността на теорията на съгласието е в познаването, зачитането и приемането на позицията на отсрещната страна във взаимовръзката гражданско общество-политическа власт.

Създадените концепции и тяхната последователност показват постепенното изграждане на гражданското общество и все по-засилващата му се роля в процесите на държавно управление.

Последната концепция е тази на толерантността. Тя се разглежда във взаимоотношенията между гражданското общество и държавата (властта). Според тази концепция, отношенията между гражданското общество и държавата се изграждат на основата на култура и ценности. Съвременните общества имат културата да водят диалог по наболели въпроси и отделните страни открито да представят своята позиция и да я защитават със средствата на нормалното общуване. Според авторите на тази инвенция, резултатите от гражданския контрол ще бъдат много по-

ползотворни, ако бъдат постигнати по един разбран и цивилизован начин. Възможността за прилагането на концепцията за толерантността в пряко свързана със степента на зрялост на гражданското общество.

II. Цели и принципи на гражданското общество и гражданските организации

Идеята за гражданското общество се базира на стремежа за реализация и защита на основните човешки социални, трудови, политически, икономически, културни и др. права и свободи. Водещ е стремежът за балансиране и уравновесяване на обществените и индивидуалните интереси. Целта на гражданското общество е да направи обществените блага достъпни за всеки гражданин. Все повече съществуването на гражданското общество се разглежда като регулатор, който не би трябва да попада под държавно влияние и контрол. Нарастващата самостоятелност на гражданското общество и разширяването на обхвата на неговите дейности се налага от динамично развиващата се и прогресивно променящата се среда през XXI век. Информационния и технологичен напредък води до развитие във всички сфери на обществения живот. Това, по естествен начин, налага гражданското общество да бъде адекватно на това развитие и да отговаря на нарастващите изисквания на все по-добре информираната и образована общност. Безпрепятствения достъп до огромен по обем информация прави манипулацията на обществото по-затруднена.

В исторически план, можем да търсим в основата на българското гражданско общество традиционните религиозни християнски патриархални традиции. Самата християнска религия изисква общността, групата да помага на нуждаещите се.

По-късно създаването на граждански обединения се обуславя от необходимостта за колективна реакция против волята на държавата.

За съвременните общества е важно гражданските обединения под формата на неправителствени и нестопански организации, фондации, синдикални организации и др. да бъдат абсолютно автономни и независими от държавните институции и да действат в рамките на закона за опазване на основните човешки права и свободи, т. е., всеки трябва да получава полагащото му се и да не се позволява на държавата да слага граници и бариери и да лишава гражданите от основните блага и потребности.

Формите на гражданските организации и обединения могат да бъдат различни в зависимост от проблемите на съответните групи. Независимо от стимула за създаването на една гражданска организация, за всяка такава са изключително важни няколко основни направления.

На първо място това е уместното заимстване на чужд опит. В годините на тоталитарния режим и особено в годините на преход, когато в нашата страна се наблюдаваше дезориентация във всяка сфера на обществения живот, България загуби много по отношение на изграждане на стабилно и добре функциониращо гражданско общество. в това време на лутане за нашето общество развиващите се и развитите страни по в Европа и по света натрупаха ценен опит. С напредването на технологиите достъпът до информация е бърз и лесен и всеки един от нас, като гражданин, би могъл да бъде полезен на обществото като почерпи опит от добрите практики по света. Гражданското общество в България би могло да последва работещите модели и да ги прилага в своята дейност у нас. В последните години не малко организации се създадоха именно на този принцип. Много от тях не бяха успешни, тъй като не всеки модел може да бъде копиран и да се окаже работещ навсякъде. По тази причина, освен пренасянето на добрите практики е редно те да

бъдат приспособени и приложени така, че да бъдат адекватни на конкретните потребности на гражданите.

На второ място това е изграждането на традиции в съществуването на гражданското общество. Често наблюдаваме периодично създаване на различни видове организации. Те съществуват в рамките на даден проект или група хора се обединява по повод възникнал процес, след приключването и решаването им организацията спира да съществува. Редно е, за да се развива и да се усъвършенства гражданското общество, като цяло, да се създават трайни и устойчиви организации, които да предават своя опит и да подобряват своята дейност в различни насоки. Няма да споменаваме тук редицата организации, които се създават с цел усвояване на европейски средства и след това въпросната организация остава само формално да съществува, не извършва дейност. Като цяло, дейността на гражданското общество следва да бъде безпристрастна и благородна и да следва основната си мисия по опазване на човешките права.

Друго направление, в което гражданското общество трябва да насочи своите действия е сътрудничеството с международни организации. В днешно време, когато границите стават все по-лесно преодолими и независимо от местоживеенето всеки отделен индивид е гражданин на света, няма по-естествено от това да си сътрудничат не само държавите като политически и икономически субекти, но и гражданите и техните организации. Живеем във време, когато човешкия живот протича на различни територии в различно време. Всеки човек трябва да може да бъде спокоен, че неговите права и свободи ще бъдат гарантирани, независимо от това в коя точка на света се намира. В България вече има не малко организации, които търсят и осъществяват международно сътрудничество. По този начин те обогатяват своята дейност и могат да бъдат много по ефективни и полезни на обществото.

Основният проблем в България е, че формално и теоретично има справедливо уреждане на въпросите свързани с функционирането на гражданското общество. Законно гражданите имат право да декларират своя избор, гражданските организации имат право да участват в управленския процес. Проблема възниква при прилагането на тези права на практика. В последните години наблюдаваме все позадълбочаваща се криза на доверие от страна на гражданите в държавата и в управляващите. Тази криза би могла да доведе или до застрашаваща апатия, която може да се окаже не само неблагоприятна, но и пагубна или до внезапен изблик на обществено недоволство. И двата варианта не са целесъобразни. Целта е да бъде постигнат баланс, който да гарантира доброто управление на държавата и удовлетвореността на нейните граждани.

Гражданското общество може да действа независимо от държавата в рамките на закона. Законите, обаче, се изработват от държавата в лицето на избраните народни представители. Те имат силата чрез изготвянето на нормативните актове да поощряват или да ограничават действията на гражданското общество. Би следвало нормативната уредба да бъде изработена така, че да удовлетворява обществото. Гражданското общество от своя страна трябва да бъде добре информирано и да не допуска държавата да стеснява границите на неговата дейност. Това би могло да стане чрез навременна и адекватна реакция по подходящ за съответната ситуация начин, при стриктно проследяване на действията на държавните органи и информираност относно подготвяните законопроекти и всяка публична дейност на държавните органи.

Обобщаването на всички граждански, неправителствени и нестопански организации в термина „трети сектор“ следва да подчертаят важността и неизменната необходимост от тези обединения във всяка демократична държава. Третият сектор заедно с държавния и частния са всъщност участниците в управленския процес. Съществуването на този трети сектор дава възможност за по-широко участие на гражданите в управлението на държавата и във всички обществени процеси, улеснява закрилата на индивидуалните и общите права и дава възможност за израстване на обществото като цяло. Следователно разнообразието на обединенията и организациите в третия сектор създава предпоставка за по-голяма устойчивост и стабилност на гражданското общество. Доброто и пълноценно развитие на гражданското общество от своя страна води до по-пълноценно прилагане на принципите на демократичното управление и се наблюдават спокойни и балансирани взаимоотношения между държавата и нейните граждани.

Много често се създават граждански организации, предимно фондации, които са с идеална цел. Техните членове не получават никакво възнаграждение или то е съвсем минимално. Тези организации, обикновено, се създават за подпомагане на някаква кауза или личност. Различни могат да бъдат причините, които спомагат човек да се отдалечи от по природа меркантилната си същност. Това могат да бъдат например религиозни причини. Едно силно вътрешно убеждение, че хората трябва да правят добро, за да бъдат в душевен мир, както учат християнската религия и етика. Друга причина за създаване на големи корпоративни фондации би могло да бъде облекчения данъчен режим и данъчните преференции, от които те се възползват.

Подбудите на всеки отделен индивид са различни и разнообразни. Важното е всеки човек да знае, че гражданското общество, както и държавата са съставени от хората и никоя от тях не може да съществува при едно непостоянно и хаотично поведение на съставните си елементи. Възпитанието на гражданското самосъзнание трябва да става у всеки човек поотделно, за да се формира и да функционира обществото като образовано информирано и защитено.

III. Третият сектор

Третият сектор е едно обобщено определение на всички граждански, неправителствени и нестопански организации. Това е гражданския сектор, съставляван от гражданите и техните обединения и в него намират израз и защита обществените потребности и права.

Когато обществото преминава своята трансформация, за да се превърне в гражданско, обществените обединения са тези, които осигуряват условията за неговото функциониране. Нестопанските организации са такива с идеална цел. Тяхната мисия следва да е да служат на обществото и да подкрепят неговите потребности, а не да се облагодетелстват чрез получаване на печалба от дейността си.

Гражданските организации имат голяма заслуга за процеса на функциониране и съществуване на гражданското общество. Сред основните им функции е ролята на компенсиращо звено, т. е., те трябва да запълват онези празноти и несъвършенства в изграждането на държавния апарат, които са липсващи или непълно функциониращи. Те стимулират обществото да насочва своите граждански усилия към преодоляване на несъвършенствата в системата на държавно управление.

Друга важна роля на организациите, съставляващи гражданското общество е да популяризират неговата дейност и да направят идеите му достъпни до възможно най-широк кръг хора. Целта е, възможно най-голяма част от обществото да бъде

приобщена към идеите и принципите на гражданското общество, да са запознати с идеалите, които то следва и по този начин максимално да подобрят дейността му.

Гражданските организации изпълняват ролята на балансьор, който уравновесява социалното неравновесие, чрез провеждането на различни дарителски кампании, подпомагане на хора или групи в тежко финансово и социално положение и др. Не винаги държавата може да задоволи жизненоважни потребности на хора в неравностойно социално положение. Именно тук е полезна намесата на организации, които намират различни начини за набиране на материални средства или осигуряване на нематериална подкрепа. В този аспект дейността на гражданските организации е от изключително голяма роля и значение за обществото.

Основен мотив за членство в гражданска организация за всеки отделен индивид е защитата на неговите права. Организациите спазват правата и свободите на гражданите и в рамките на закона реагират на всеки опит на държавен орган или институция по някакъв начин да ги накърни.

Целта на функционирането на гражданските организации и е да се приложи на практика демократичната форма на управление чрез прилагане на ценности и идеали, присъщи на гражданското общество, също така опазването на основните права и свободи полагащи се по рождение на всеки индивид, възпитаване на обществото в духа на вековни традиции и насочването на хората към морално и етично поведение.

За постигане на своите цели гражданското общество се оповава на демократичните ценности и идеали. За постигането на поставените цели е необходимо да се спазват някои принципи. Един от тях е този за доброволното и по желание членство в гражданските организации. Всеки отделен индивид има право да се обръща, да членува или да участва или да не участва в определени обществени групи. Всяка гражданска организация е съставена от доброволно присъстващи и членуващи и всеки може да избира една или няколко организации, които отговарят на неговите интереси и не трябва да бъде принуждаван за своето участие. Членуването в която и да е организация е израз на индивидуалното и непринудено решение на всеки отделен индивид.

Друг принцип при функционирането на гражданските организации е безвъзмездното ползване на благата, които предоставят. Напоследък се появяват организации, които предлагат защита на нуждаещ се гражданин, в замяна на което изискват определено заплащане. По принцип гражданското общество би трябвало да осъществява своята дейност безвъзмездно, с цел постигане на социално равенство и равен достъп на всеки индивид до неговите услуги и подкрепа в определена ситуация.

По принцип, отчетите от дейността на гражданските организации би следвало да имат публичен характер и да бъде осигурен достъп на всеки до тях. Тъй като началната идея на гражданското общество е да защитава, а не да ощетява обществото това не е изрично задължително, защото гражданското общество съществува и функционира предимно чрез доброволното участие и доверие на гражданите в неговата почтеност и добронамереност.

Прогресивното развитие на третия сектор е предпоставка за изграждане на балансирано, модерно гражданско общество, което да насочва гражданската енергия към постигане на добри резултати за неговото съществуване. Наличието на добре функциониращи граждански организации дава възможност за решаване на важни социални проблеми, за отменяне или допълване на държавните функции в определени области, където се забелязва недостатъчна ефективност и др.

В последните години, благодарение на техническия и информационния напредък, все повече се увеличава гражданската инициативност и желанието на обществото да покаже своята реакция и несъгласие по важни въпроси от дневния ред. Задачата на гражданското общество е да акумулира тази гражданска енергия и да я насочи в посока на постигане на най-добрите резултати и да овладее рисковете от гражданско неподчинение.

IV. Свободата и правото в правовата държава

В последните 25 години страната ни е изправена пред редица предизвикателства. Желанието за приемане на демократичния режим поставя обществото пред трудности във всяка сфера на обществения живот. Посоката на евроинтеграция е най-правилния път, който България избра. Интеграцията ни в една общност с големи перспективи дава възможност за много по-добро развитие и бъдеще за държавата и нейните граждани в частност. Сътресенията, които българският народ преминава- политически, икономически, социални и др., дават своето ежедневно отражение. Липсата на равновесие в началото на прехода стана причина страната да изостане сериозно в доста области. Присъединяването ни към Европейския съюз наложи провеждането на редица реформи. Една от основните провеждани реформи, която има пряко отношение към съществуването и развитието на гражданското общество е правната. Българското законодателство следва да бъде адаптирано към европейското. Именно добрата правна система би могла да бъде гарант за доброто функциониране на гражданското общество и формирането на правовата държава.

Правото е основен балансьор в отношението правова държава- гражданско общество в условията на демократичен режим. За да бъдат определени държавата и обществото като правови такива, правото трябва да носи характеристики като справедливост, свобода, нравственост, естествени права, правосъзнание и др. Като нормативен регулатор, правото притежава качеството легитимност, което, от своя страна, придава на правовата държава и гражданското общество. Правото е основен носител на правовата държава и неизменен компонент за формирането на гражданското общество. В България е необходима реформа не само на изготвянето на правната система като цяло, но и на методите и начините за нейното прилагане. Извършването на правната реформа следва да бъде съответно конкретната необходимост от нея. Тя трябва да бъде цялостна и всеобхватна и да засегне всички отрасли на правото. Целта на тази реформа е да бъде пригодена остарялата и трудно приложима българска правна система към съвременните европейски и световни изисквания, за да бъде в полза на обществото в реално време. При наличието на свободно гражданско общество правото създава равенство в отношенията между отделните индивиди. В условията на демокрация правото трябва да съответства на интересите на обществото, както и да предоставя равен избор за всеки гражданин. Като основа на правовата държава гражданското общество се изгражда така, че да бъде полезно за всички. Развитието на гражданското общество ще води все повече до засилване на неговия социален характер и полезността му за всеки поотделно и за обществото като цяло. Когато гражданското общество е слабо и потискано, то се превръща, по-скоро, в ограничаващ фактор на човешките свободи и става предпоставка за засилване на административната зависимост, което води до затруднено или нулево саморазвитие на обществото. Свободата е основното качество на гражданското общество, което определя демократичността в осъществяването на държавната власт. Роля на Конституцията, като основен закон на държавата, е да оп-

редели границите на свободата и правото, които се полагат изначално на всеки отделен индивид и да не могат да бъдат промени от текущи нормативни промени в законодателната сфера. Това следва от факта, че този основен закон трябва да бъде за едно свободно и силно гражданско общество, а не за услуга на държавната и политическа власт. В последните години наблюдаваме интензивен процес на световна интеграция на политическите, икономическите и социалните отношения между отделните държави. Тази международна социализация засяга и гражданското общество и налага да бъде осъществена адекватна реформа и на международното законодателство, която да съответства на интернационалното развитие на отделните страни. Трябва да се даде възможност за изграждане на отношения между гражданските общества без намесата на държавата. В последните години се задълбочават международните връзки между отделните страни. Това налага осъществяването на адекватна правна реформа, особено в областта на международното право, отнасящо се до регулиране на отношенията между гражданските организации в отделните държави. За по-лесното изграждане на отношенията между гражданското общество у нас и в страните по света, е необходимо участието на България във все повече международни договори и нормативни актове. Основна цел на правната реформа като цяло е да отъждествi българското законодателство с международните правни норми. Това е важно условие за пълната интеграция на страната ни във всяко отношение и сфера на обществения живот.

Важна част от правната реформа, като цяло, е тази в областта на административното право. Нейна цел е законодателството да бъде изградено така, че да се осъществи основното конституционно задължение на администрацията да служи на народа и всичките й действия да се ръководят от волята на народа. Това се налага от основната черта на правовата държава народът да бъде единствен източник на властта. Правовата държава предоставя широкообхватни и обемни мерки за реакция, контрол и противодействие на административния произвол, тъй като основния принцип е да бъдат опазвани основните човешки права и свободи. Правната реформа следва да доведе системата на правото в страната до основното- подчинение на цялата държавна власт и администрация на основния суверен- народа и гражданското общество, като представител и защитник на обществените интереси. По този начин, законодателството предоставя независимост на гражданското общество от държавата и администрацията. Административното право е важна част от правната система, тъй като то е основен гарант за спазване на свободата и правата на гражданите и техните организации.

Гражданското право също трябва да бъде компонент на цялостната правна реформа с цялата му всеобхватност и обвързаност с всички сфери на обществения живот.

Важна част от правната реформа е и наказателното право. То се отнася до определянето и прилагането на справедливи и адекватни методи и мерки за отговорност и наказание при установяване на различни нарушения и неправомерности.

Основните компоненти на правната реформа, като цяло, са няколко основни направления и важността на всеки един от тях е от изключително значение. Реформата трябва да бъде цялостна, всеобхватна и адекватна, а не да засяга само отделни елементи.

Реформата трябва да включва компоненти като: конституционна реформа- като основен закон в държавата, Конституцията трябва да обхваща и отразява промени-

те във всички сфери на нормативния процес; изграждане на ново либерално частно право и качествено ново публично право; реформа в областта на международното право- публично и частно с цел уеднаквяване на нормативната база на взаимодействащите си страни; реформа в областта на административното право, с цел да бъде изградена административна система, чийто действия да бъдат изцяло насочени в името и в полза на обществото; гражданско правна реформа във всички аспекти на неговото приложение и др.

При провеждането на всеобхватна реформа на цялата правна система, всяка промяна трябва да бъде изключително добре подготвена и да се извършат всички необходими проучвания. В процеса на присъединяване към Европейския съюз в България бяха извършени редица промени, за да отговори на изискванията, включително и в областта на правото. Тези реформи продължават и ще се налагат, тъй като във всички сфери се наблюдават динамични промени, които всяка страна, в това число и България, трябва да отразява, за да бъде адекватна на моментните изисквания. Правовата държава е политическата основа на гражданското общество. Правната система като неин компонент следва да бъде изградена така, че във всяка една област да действа в защита на обществените интереси.

V. Мястото на медиите в отношенията между гражданското общество и държавата

В съвременните общества е изключително важно мястото на медиите като участник и посредник в отношенията и комуникацията на обществото и държавата. Основната им роля е да бъдат безпристрастен информатор за случващото се в държавата и да предоставят обективна информация дейността на институциите и управляващите. Те могат да бъдат сериозна подкрепа на гражданското общество и да подпомагат различни граждански прояви. Благодарение на властта, която имат, често се случва да се злоупотребява и медиите да се превръщат по-скоро в манипулатор и да насочват масовото мнение и възприятие по наболели въпроси в определена посока. Често се случва различни печатни или електронни медии са се опитват да насочват обществото в посока, отговаряща по-скоро на техните лични и индивидуални интереси, и да изместват дейността си от основния фокус на тяхната значимост, а именно да информират обществото реално и да пренебрегват собствените си облаги. Също така, непрекъснато се появяват обвинения, че различни медии обслужват определени политически и икономически интереси. Това е една от причините в последните години в България на медиите да се гледа с известно недоверие от страна на гражданите. Всеки гражданин има правото да получава безпристрастна и обективна информация. Понякога в защита на интереси, които не са в полза на обществото се дава акцент на случващо се с по-маловажно значение, за сметка на прикриване или непълно представяне на важна информация. В такива случаи се възпрепятства възможността на гражданското общество да реагира и да изрази своето мнение по дадения въпрос, което лишава определена група индивиди или обществото като цяло от правото си да участва в управленския процес. Друг основен проблем по отношение на медиите у нас е, че в последните години бяха създадени голям брой частни телевизии и радиостанции, в пресата също излизат редица нови издания, а също и необятните информационни агенции в интернет пространството. Това до голяма степен води до една чисто корпоративна конкуренция между отделните медии или личностни сблъсъци между техните управители, което много често отдалечава дейността им от основната им функция и гражданите стават жертва на тези взаимоотношения. Това създава и проблема на претоварването и пренасищане с информация и объркване на обществото.

В последните години в българското медийно пространство все повече се утвърждава т. н. „разследваща журналистика“. Чрез нея се дава възможност по още един, в повечето случаи доста успешен начин, да бъдат защитавани правата и интересите на гражданите от неправомерни действия или бездействие от страна на администрацията. Разследванията се осъществяват самостоятелно от журналисти или от екипи, които провеждат продължителни проучвания за събиране на доказателства по различни наболели въпроси. Даването на гласност на въпроси, които е имало стремеж да бъдат прикрити и неоповестявани в много от случаите дава основание на институциите да предприемат мерки за тяхното решаване. Най-често, проблемите, които са обект на разследващата журналистика са свързани с корупция на различни нива, злоупотреба с власт, прикриване на незаконни действия с цел лични облаги и др. В това отношение медиите играят важна роля и оказват сериозна подкрепа на гражданското общество за справянето с проблеми, които са в ущърб на населението.

Определянето на медиите като „четвърта власт“ показва важността им във всички сфери на обществения живот. Също така не бива да се пренебрегва тяхната сила и възможност за насочване контрол, а в много случаи манипулация на общественото мнение. Те имат властта и способността да насочват общественото внимание в определена посока и така да влияят върху цялостното възприемане на даден проблем.

Не е тайна и съществуването на партийни телевизии и печатни издания. Те защитават партийни интереси и не могат да представят обективно събитията тъй като ги отразяват през призмата само на една гледна точка.

Ролята и важността на медиите е безспорна. Особено в нашето съвремие, когато хората имат все по-широки възможности за достъп до информация и се възползват от правото си да следят случващото се и управлението и да изразяват своето мнение и участие във важни за страната или за отделните индивиди въпроси. За съжаление, нерядко медиите си позволяват да злоупотребяват с тази власт и да нарушават правото на точна и безпристрастна информация. Наличието на голям брой медии- електронни и печатни създава конкуренция между тях и до голяма степен това може да бъде в полза на обществото тъй като ги стимулира да работят по ефективно и да поднасят достоверна информация. Наличието на много и различни медии стимулира управляващите, администрацията и институциите да осигуряват максимална прозрачност в своята дейност. Присъствието на медиите е задължителен елемент в отношенията между държавата и гражданите и в много случаи те могат да оказват сериозна подкрепа на гражданското общество в борбата за защита на основните човешки права и граждански интереси.

Заключение

Понятието „гражданско общество” отразява етап от развитието на обществото като цяло. Характерно за обществото, което се нарича „гражданско” е едно ново ниво на отношенията между отделните личности, групи, етноси, народности, религии, класи, раси, които го съставляват. В процеса на развитие и еволюция на света хората успяват да се организират, създавайки държави, едновременно с развитието на буржоазното общество, което се разглежда като начална форма на гражданско общество.

Гражданското общество е обект на изследване от теорията още от античността, но в този етап то се разглежда по-скоро в политически аспект. Понятието „гражданско общество” преминава различни етапи на развитие, за да се достигне използването му в наши дни като определящо съвременната социална, икономическа и правна теория.

ЛИТЕРАТУРА

1. Проданов, В., Гражданското общество и глобалният капитализъм, С., 2003.
2. Селигман, А., Идеята за гражданското общество, С., 1995.
3. Стоянов, Ж., Глобализация и гражданско общество, С., 2012.
4. Dicken, P., Global Shift, New York-London, 2004.
5. Drucker, P., Post-Capitalist Society, New York, 2005.
6. Etzioni, A., The Spirit of Community Rights, Responsibilitiesq and The Communitarian Agenda, New York, 2003.
7. Giddens, A., Beyond Left and Right, The Future of Radical Politics, Cambridge, 2006.
8. Giddens, A., The Third Way and the Critics, Cambridge, 2004.
9. Inglehart, R., Culture Shift in Advanced Industrial Society, New York, 1998.
10. Kean, J., Civil Society: Old Images, Cambridge, 2003.
11. Kean, J. ,(Eds.), Civil Society and the State, London, 1988.
12. Rifkin, P., The End of Work, The Declibe of the Global Labour Force and the Dawn of the Post-Market Era, New York, 1999.
13. Saunders, F., The Cultural Cold War: The CIA and the World of Arts and Letters, New York, 1999.
14. Shaw, M., Global Society and International Relations. Cambridge, 1998.

СТАБИЛНОСТ И ИЗМЕНЧИВОСТ В ОРГАНИЗАЦИОННИТЕ ЦЕННОСТИ

Майяна Митевска-Енчева

Университет по библиотекознание и информационни технологии, София

STABILITY AND VARIABILITY OF ORGANIZATIONAL VALUES

Mayiana Mitevska-Encheva

***ABSTRACT**:* An analysis of the impact of a number of demographic indicators on organizational climate is presented. The survey results make it possible to reveal the trends in the development and the change of organizational climate. The hypotheses check is performed by ANOVA dispersion analysis. Data have been processed with the standard package of statistical programs SPSS-16.

***KEY WORDS**:* organizational climate, demographic variables

Увод. Стабилността и изменчивостта на доминиращите ценности се разглежда в аспекта на изследването на организационния климат. Анализира се наборът от устойчиви характеристики, които влияят съществено върху поведението и емоционалното състояние на членовете на организацията. Използват се следните параметри за описание на организационния климат: демографски признаци – пол, възраст,

образование, статус и др; структурата на организацията; възможността за кариерно развитие; отношението на ръководството към служителите; отношението на служителите към ръководството; емоционално-психическата атмосфера и др. Като синоними на организационният климат се използват и словосъчетанията: социално–психологически климат, производствен климат.

Така, изведената променлива „организационен климат“ формулира **основната цел** на изследването – установяване на влиянието на феномени от организационно и демографско равнище върху организационния климат. **Очаква се** по този начин да се потвърди допускането, че организационния климат изпълнява определена значима роля в организацията. Базирайки се на влиянието на изброените променливи се издига **хипотезата**, че ще бъдат изведени конкретни различия, които да очертаят профила и спецификата на психологическия климат на работното място. Респондентите на изследването са над 100 лица, работещи студенти и преподаватели.

Метод за психологическо изследване. Използваният метод е Въпросник за организационния климат на Van Muijen at al. [7]. Твърденията са 40 и се измерват по 6-степенна скала на Ликърт. Инструментариумът е адаптиран за български условия от С. Илиева [1] и показва високи психометрични качества. Измерват се четири типа климат, ориентирани съответно към подкрепата, иновациите, целите и правилата. *Иновационният климат* показва търсенето на нови решения, *климатът на подкрепата* се изразява в доверие и сътрудничество, *климата на правилата* разглежда координацията вътре в организацията,а *на целите* се характеризира с решаване на задачите на работното място. С „x” се означат средностатистическите стойности, с „sd” – стандартното отклонение.

Допуска се, че организационният климат, като пряко и дълбинно свързан с поведението и преживяванията на хората на работното място, формира перцепциите към определена ценностна ориентация. Според данните от дескриптивната статистика (Фиг. 1) ясно се извеждат ценностните предпочитания към климата на правилата (x=4.41; sd=0,57) в ролята си на доминиращи спрямо ценностите на останалите типове организационен климат.

Табл. 1. Дескриптивна статистика на видовете организационен климат

Организационен климат	X	SD
Климат на иновациите	3.71	0.73
Климат на подкрепата	3.90	0.99
Климат на правилата	**4.25**	**0.81**
Климат на целите	4.07	0.81

Респондентите възприемат своята работа като изпълнена с много правила, които трябва да се следват прецизно. Така, от една страна се изявява потребността на служителите от стабилност, но от друга, вероятно е знак за ниска степен на гъвкавост спрямо динамичните условия, които подсказва външната среда.

След доминиращите ценности на консерватизъм, единство в нарежданията и съобразяване с властта и авторитетите се нарежда яснотата при изпълнението на поставените задачи, точно измерване на изпълнението и приемане на лична отговорност за извършената работа и служебните задължения (x=3,84; sd=0,93). Акцентът е поставен върху формалната комуникация и формализацията. Той улеснява

изпълнението, но застрашава ефективността, иновативността и ориентацията към ценностите на подкрепа в работата.

За разкриване на различията във възприятията на видовете организационен климат е направен **многофакторен дисперсионен анализ** в зависимост *от пола, възрастта, стажа в организацията, общия трудов стаж, броя на членовете в групата, образованието и позицията в йерархията.* Основанията за това са, че перцепциите за видовете на организационния климат се влияят и от изброените променливи. Целта е да се изведат онези средни аритметични стойности, които са статистически значими. Тъй като се допуска, че тези различия са по-изразени между някои от групите изследвани лица е използван и Post hoc Тест за множествени сравнения, направен по метода на Tukey. Тестът за множествени сравнения се прилага след като се установи след еднофакторния дисперсионен анализ ANOVA, че F-отношението е значимо, „p" е равнището на значимост, не по-голямо от 0,05.

Очаква се да съществуват и различия по независимите демографски променливи *пол, възраст, конкретен стаж в организацията, общ трудов стаж, брой на членовете в групата, образование и позиция в йерархията.* Те биха могли в дълбочина да очертаят сигурността и кризата във възприемането на доминиращите ценностни ориентации. В този смисъл се допуска хипотезата, че според променлива **пол** ще се наблюдават различия в ориентацията към иновациите и целите, търсенето на подкрепа и разбиране. Основанията за това са, че перцепциите за за типа организационен климат се влияят от чисто индивидуалните променливи като пол и възраст. Полът обаче не оказва статистически значими влияния върху възприятията на респондентите. Може да се предполага за липсата на стабилност при полово-ролевите функции, отчасти и заради честите промени във външната икономическа среда.

Възрастовите различия определят статистически значими показатели (вж. Фиг. 2.) при климата на подкрепата ($F=3,42$; $p=0,02$) и на целите ($F=2,45$; $p=0,05$).

Дисперсионният анализ показва, че най-силно се изявява ориентацията към подкрепящ климат при служителите на възраст от 26г. до 35г. ($x=4,05$; $sd= 0,80$), както и при тези от 36г. до 45г. ($x=3,85$; $sd=1,07$), следван от тези на възраст над 45г. ($x=3,46$; $sd=1,06$). Най-слаби са ориентациите към климата на подкрепата при служителите до 25г. ($x=3,85$; $sd=1,07$).

По принцип се приема, че иновационно поведение може да се формира като поддържането на климат на подкрепата и създаването на чувство за сигурност на работното място. Така една атмосфера, изградена на базата на доверие и сътрудничество между членовете на организацията в по-голяма степен може да изяви творческите нагласи у служителите, което от своя страна да повлияе и върху креативността и инициативността.

Тестът за множествени сравнения показа слабо диференциращо значение при групите на възраст до 25г. с групите на възраст до 35г., ориентирани към климата на подкрепата. Най-ниските стойности за този тип климат са рестрирани при служители на възраст до 25г., а най-високи при изследваните лица до 35г. така организацията се възприема от по-младите като място, на което първоначално стартират своята кариера, без да го очакват професионално развитие там.

Ориентацията към изпълнението на организационните цели е най-силно поддържана от служители на възраст до 45г. ($x=4,13$; $sd=1,00$), както и от служители до 35г. ($x=4.00$; $sd=0,65$). Най-ниски стойности се отчитат при възрастовата група над

45г. При служителите до 25г (x=3,73**;** sd=0,81) се наблюдава криза при изповядването на организационните виждания като свои. Според данните от теста за множествени сравнения не се регистрират различия между възрастовите групи при климата на целите.

Табл. 2. Различия във възприятията на видовете организационен климат според възрастта

Организационен климат	*Възраст*	*x*	*sd*	*F*	*p*
Климат на иновациите	*до 25 г.*	3.27	0.66	1.33	0.270
	до 35 г.	3.72	0.66		
	до 45 г.	3.57	0.82		
	над 45 г.	3.38	0.87		
Климат на подкрепата	*до 25 г.*	3.14	0.69	**3.42**	**0.021**
	до 35 г.	**4.05**	**0.80**		
	до 45 г.	3.85	1.07		
	над 45 г.	3.45	1.06		
Климат на правилата	***до 25 г.***	4.02	1.01	1.67	0.179
	до 35 г.	4.25	0.66		
	до 45 г.	4.24	0.10		
	над 45 г.	3.80	0.91		
Климат на целите	***до 25 г.***	3.73	0.81	**2.44**	**0.050**
	до 35 г.	4.00	0.65		
	до 45 г.	**4.13**	**1.01**		
	над 45 г.	3.56	0.99		

Нивото в йерархията е диференциращ фактор за организационна подкрепа (F=4,56; p=0,04) с най-високи данни при ръководството (x=4,19; sd=0,07). Доминиращите ценности за следването на правилата (F=3,71, p=0,05) отново с по-ясна изразеност при заемащите ръководни позиции (x=4,25; sd=0,87).

Табл. 3. Различия във видовете организационен климат според йерархичното ниво

Организационен климат	*Йерарх. ниво*	*x*	*sd*	*F*	*p*
Климат на иновациите	*Ръководител*	3.57	0.76	0.81	0.37
	Изпълнители	3.43	0.81		
Климат на подкрепата	***Ръководител***	**4.19**	**0.07**	**4.60**	**0.04**
	Изпълнители	3.46	1.06		
Климат на правилата	***Ръководител***	**4.23**	**0.87**	**3.71**	**0.05**
	Изпълнители	3.90	0.93		
Климат на целите	*Ръководител*	3.99	0.93	1.95	0.17
	Изпълнители	3.73	0.91		

Сигурността на работното място се поражда от поддържането на ценности и норми на поведение като лоялност и привързаността към организацията. В същото време ориентацията към правилата показва заинтересованост в следване на точните правила и ясните процедури, контролът върху дейността, както и съхраняването на статуса и вътрешната стабилност в организацията. В този смисъл предпочитаните ценности представляват симбиоза от вътрешна интеграция и сплотеност, от една страна, и гъвкавост и динамичност, от друга, с акцент върху развитието на човешкия потенциал. Тези ценности са поддържани от ръководителите.

Общият трудов стаж е диференциращ фактор (вж.Фиг.4) при два от четирите типа организационен климат - ориентиран към правилата (F=3,75, p=0,03) и ориентиран към целите (F=3,09, p=0,05). При климата на иновациите и при климата на подкрепата не се констатират статистически значими показатели в зависимост от стажа. При служителите с трудов стаж до 15г. се проявяват най-силно ценностните предпочитания добри междуличностни отношения в организацията (x=4,36; sd=0,73) за координация на изпълнението на организационните задачи (x=4,12; sd=0,73).

Табл. 4. Различия във видовете организационен климат според общия трудов стаж

Организационен климат	*Общ стаж*	*x*	*sd*	*F*	*p*
Климат на иновациите	*До 5г.*	3.50	0.70	1.83	.165
	До 15г.	3.70	0.73		
	Над 15г.	3.34	0.86		
Климат на подкрепата	*До 5г.*	3.63	0.85	1.15	.320
	До 15г.	3.87	0.87		
	Над 15г.	3.51	1.16		
Климат на правилата	*До 5г.*	4.11	0.91	**3.75**	**.027**
	До 15г.	**4.36**	**0.73**		
	Над 15г.	3.79	0.97		
Климат на целите	*До 5г.*	3.92	0.83	**3.09**	**.050**
	До 15г.	**4.11**	**0.73**		
	Над 15г.	3.60	1.04		

Налице е тенденция с нарастване на стажа до 15г. да се оценяват качествата на емоционално-психологическата атмосфера на работното място. Над 15г. общ трудов стаж служителите предпочитат сигурността, стабилността и отклоняват предложения, свързани с висока степен на риск. Данните от многофакторния дисперсионен анализ дават основание да се изгради профил за групите служителите: ценят повече реда, сигурността на работното място, спазват формалните процедури и са предразположени към умереното въвеждането на промяна. Иновационно поведение на работното място се приветства, като не се загърбват традициите и добрия

опит. Според данните пазарно-ориентираните промените се въвеждат от служителите със стаж до 5г. В същото време тези служители в не по-малка степен уважават установения ред (x=4,12; sd= 0,91) и принципи на работа (x=3,92; sd=0,83).

Според данните от многофакторния дисперсионен анализ изследваните лица със стаж над 15г. придават значение на рутинността (x=3,80; sd=0,97), придържат се към точно определени методи на работа и избягват риска (x=3,51; sd= 1,04).

Тестът за множествени сравнения отчита различия между групите до 15г. – с над 15г. общ трудов стаж. Установи се, че общият трудов стаж е променлива, която влияе върху пазарната ориентация и изборът на йерархичността в организационните структури като надежден начин за оцеляване.

Извеждат се статистически значими показатели по самостоятелната променлива **„стаж в конкретната организация“** (вж. Фиг.5) при климат, ориентиран към целите (F=2,46; p=0,03), като най-изразени предпочитания към този тип ценностна градация се анализират при служителите със стаж на конкретното работно място до 4г. (x=4,31**;** sd=0,81), следвани от до 2г. (x=3,83**;** sd=0,89) и над 4г. (x=3,76**;** sd=0,95).

Табл. 5. Различия във видовете организационен климат според стажа в конкретната организация

Организационен климат	*Конкр. стаж*	*x*	*sd*	*F*	*p*
Климат на иновациите	*До 2г.*	3.54	0.82	0.11	0.90
	До 4г.	3.54	0.63		
	Над 4г.	3.46	0.81		
Климат на подкрепата	*До 2г.*	3.69	1.02	0.08	0.92
	До 4г.	3.55	0.84		
	Над 4г.	3.64	1.04		
Климат на правилата	*До 2г.*	4.06	0.94	0.88	0.42
	До 4г.	4.38	0.73		
	Над 4г.	3.99	0.94		
Климат на целите	*До 2г.*	3.83	0.89	**2.46**	**0.03**
	До 4г.	**4.34**	**0.81**		
	Над 4г.	3.76	0.95		

Стажът в конкретната организация е диференциращ фактор по отношение на пазарната ориентация. Основните ценности, които се поддържат са желанието за продуктивност, постигане на високи конкурентни нива, отговор на потребностите на „потребителите на продукта“ и добрата обратна връзка при респондентите със стаж до 4г. без промяна на работно място.

Тестът за множествени сравнения не отчита различия между изследваните групи. Репутацията и успехът са еднакво значими за всички изследвани лица. Служителите се конкурират помежду си и се стремят към постигане на поставените по

план цели. Въз основа на данните от многофакторния дисперсионен анализ респондентите намират сигурност във външното пазарно ориентиране.

Отчитат се статистически значими показатели според променливата **„брой членова в групата”** (вж. Фиг.6.) за ценностната ориентация към иновациите (F=3,494; p=0,050), правилата (F=3,22; p=0,05) и целите (F=4,41; p=0,04). Резултатите от многофакторния дисперсионен анализ сочат, че групите над 10 души са диференциращ фактор изброените доминиращи организационни ценности.

Табл. 6. Различия във видовете организационен климат
според броя на членовете в групата

Организационен климат	*Брой членове в гр.*	*x*	*sd*	*F*	*p*
Климат на иновациите	*До 10 души*	3.37	0.82	**3.49**	**0.05**
	Над 10 души	**3.70**	**0.68**		
Климат на подкрепата	*До 10 души*	3.64	1.06768	0.01	0.94
	Над 10 души	3.66	0.88		
Климат на правилата	*До 10 души*	3.93	0.92	**3.22**	**0.05**
	Над 10 души	**4.28**	**0.85**		
Климат на целите	*До 10 души*	3.70	0.91	**4.41**	**0.04**
	Над 10 души	**4.11**	**0.92**		

Установените различия подчертават като основна характеристика на екипната дейност сплотеността, лоялността и ангажираността към изпълнението на поставените цели. Според изведените данни изследваните лица разглеждат работа си като взаимодействие между партнъори чрез стимулиране творчески капацитет. В същото време се подчертава важната роля на традицията, имайки предвид статистически значимите резултати на климата на правилата, аналогични с данните на климата на иновациите. И така, поемането на рискове и търсенето на нови идеи е на базата на преосмислянето и преобразуването на старите идеи и правила.

Изводи. Въз основа на получените резултати при дисперсионния анализ може да се обобщи, че демографските показатели до голяма степен диференцират различията в перцепциите към доминиращите ценностни ориентации. Установените статистически различия очертават спецификата на възприятията на видовете организационен климат. Резултатите от многофакторния дисперсионен анализ, показват, че стажът в конкретната организация най-силно диференцира типовете организационен климат и определя пазарната насоченост на респондентите. Общият трудов стаж извежда статистически значими стойности най-вече при ценностите, ориентирани към правилата и към целите. Статусът на работното място е диференциращ фактор за подкрепата и правилата. Независимата променлива „възраст“ извежда различия спрямо ценностите на подкрепата и целите. Образованието и възрастта са диференциращ фактор към всеки тип климат с изключение на подкрепата. Броят на хората в трудовата група оказва диференциращо значение за иновациите, спазването на правилата и приобщаването към организационните цели.

От получените резултати може да се направи заключението, че всяка една от независимите променливи оказва в различна степен влияние върху типовете организационен климат. Констатира се, че полът не е диференциращ фактор за типа организационен климат. Този факт може да бъде обяснен с предимството на хомогенни по пол трудови групи.

Най-много вариации са изведени при организационния климат насочен към целите. Резултатите от многофакторния дисперсионен анализ показват, че най-силна диференциация се регистрира към ценностите, които поддържат конкурентоспособността, продуктивността, постигането на високи резултати и печалби и умереното поемане на рискове. Основният фокус е върху отчитането на потребностите на потребителите и постоянните и чести контакти с тях. В същото време се установяват голям брой вариации и при климата на правилата, точните, ясните процедури и ориентацията към вътрешния фокус, целяща поддържането на стабилност и цялост на организацията. Доминиращите ценности на иновационното поведение са изведени според всяка една от изследваните независими променливи - ценят се качествата, свързани с творческите и предприемаческите нагласи, новаторството и изобретателността. Представените анализи могат да помогнат за диагностициране на ценностните предпочитания в органазационата среда.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Илиева, С. Организационна култура. - София: Унив.изд. Св. Кл. Охридски, 2006

2. Илиева, С. Ценности и трудова мотивация– София: Унив.изд. Св. Кл. Охридски, 2011, 375с.

3. Карабельова, С. Ценности и културни практики в България - София : Класика стил, 2011.

4. Карабельова, С. Управление и развитие на човешкия потенциал. – София : Класика стил, 2004.

5. Майяна Митевска-Енчева, Просоциално поведение и организационен климат, София, За буквите 2013, 201 с. ISBN 978-954-2946-75-5

6. Паповян, С.С. Исследования „организационного климата“ в американской психологии // Вопросы психологии. 1978, N2, с.163–170; по Katz.D., Kahn.R. The social psychology of organizations. N.Y., 1966.

7. Van Muijen, J.,Koopman, P., De Witte, K., De Cock,G., et al. (1996). The FOKUS-instrument for measuring organizational climat in nine European Languages. 14th Newsletter of the International research group FOCUS.

СИГУРНОСТ И КРИЗА В ДОМИНИРАЩИТЕ ЦЕННОСТНИ ПРЕДПОЧИТАНИЯ В ОРГАНИЗАЦИОННА СРЕДА

Майяна Митевска-Енчева

Университет по библиотекознание и информационни технологии, София

SECURITY AND CRISIS IN THE DOMINANT VALUE ORIENTATIONS IN ORGANIZATIONS

Mayiana Mitevska-Encheva

ABSTRACT: The research uses a comparative approach to identify the stability and variability of organizational values in different areas of activity. Data have been processed with the standard package of statistical programs SPSS-16.

KEY WORDS: *organizational values, culture, conflicts*

Увод

Най-често посочваните средства за формиране на организационна сигурност са традициите, церемониите, ритуалите, разказите, митовете и легендите. Чрез тях е възможно сближаването на хората в една трудова общност. Част от тези средства се прилагат целенасочено като начини за изграждане на определен тип доминиращи ценностни ориентации. Промените в доминиращите ценности на работното място могат да доведат до съществени кризи. В подобни ситуации организационната среда се оказва и конфликтна - нарушава се разбирането и изпълнението на организационните цели. Но конфликтите и кризите се отличават с двойнствена природа – крайният им резултат може да бъде и полезен, и вреден за организацията, а може и да формира оптимална структура на организационното управление.

В изследването се анализира настоящото състояние и възможните перспективи за развитие на организационната култура, както и на типовете конфликти и стилове за разрешаването им като показател за състоянието на доминиращите ценностни ориентации.

Обект на изследването е организационната култура в шест различни сфери на дейност. Предмет на изследването е влиянието на организационната култура върху конфликтите и стилове за разрешаването им. Целта на изследването е да се разкрие взаимното влияние на доминиращия тип организационна култура, видовете конфликти и стратегии за разрешаването им в различни сфери на дейност.

Използвана е комбинацията от следните основни изследователски **методи:**

- **Апробиран диагностичен инструментариум за изследване на организационната култура „ФОКУС**“ [1], където организационната култура, се възприема като модел на конкурентни ценности, включващ четири ценностни ориентации: към целите, към подкрепата, към иновациите и към правилата. Отделните измерения на организационната култура се съдържат в 35 твърдения. Използва се шестстепенната скала на Ликърт, която варира от „никога“ до „винаги“. Надеждността на

въпросника е много висока (α=0.86), като отделните подскали показват добра надеждност според коефициента α на Кронбах и са сходни с резултатите и на други изследователи, които са прилагали въпросника [3; 4].

- Инструментариумът за конфликти и стратегии за разрешаването им, разработен под ръководството на Рахим Афзал. **Използваната анкета [5], разпределя типовете конфликти** на три вида: междугрупов, вътрешногрупов и ролеви. Съставена е от 21 твърдения, които разкриват съответно наличието или липсата на конфликти. За всеки тип конфликт са зададени по 7 твърдения като между тях има и реверсивни. Оценките се дават по 5-степенна скала на Ликърт, започвайки от 1 – напълно не съм съгласен до 5 – напълно съм съгласен. Надеждността на въпросника е много висока (α=0.89). Отделните подскали показват добра надеждност според коефициента α на Кронбах. **Въпросникът за разрешаване на конфликти [6],** разглежда пет стила в зависимост от ориентацията към себе си или към другите, като се прилага разбирането, че няма най-добър стил, изборът зависи от това, с кого в йерархията на организацията е конфликтът - с ръководството, с колегите, с подчинените. Инструментариумът се състои от 35 твърдения, съответно описващи интегриращия, избягващия, доминиращия, услужливия и компромисния стил.
- Приложени са редица статистически методи, които дават възможност да се оцени степента на влияние на факторите, както и да се определят онези от причините, които имат съществено значение. Използва се регресионен анализ. Очаква се чрез посочените методи да се разкрие спецификата на ценностите, провокиращи сигурност и криза в организационната среда на шест различни сфери на дейност: информационни технологии (ИТ), мехатроника и автоматизация (МА), научно-изследователска (НИД), търговска, издателска и библиотечна. Данните са обработени със стандартния пакет статистически програми SPSS-16.

Застъпва се основната хипотеза, че организационната култура, която се характеризира с избора на ценностна ориентация би оказвала пряко влияние върху типовете организационни конфликти и стратегиите за разрешаването им. Основанията за това са, че те са най-силните и предиктивни фактори, които ясно могат да я определят. Очаква се по този начин да се потвърди предположението, че организационната култура и конфликти изпълняват важна роля в организацията. Допуска се също така, че действието на различните типове организационна култура влияе върху определени видове конфликти и стратегии за разрешаването им.

Извадка. Респондентите надвишават 100 човека за всяка една от изследваните групи за периода 2009г. - 2011г. и са разпределени според демографски признаци. Жените (63,3%) са приблизително два пъти повече от мъжете (36,7%). В зависимост от заеманата позиция в организацията мениджърите са 15,8%, а изпълнителите – 84,2%. Според стажа в конкретна организация респондентите са разпределени в три групи: до 2 г. – 35,5%, до 4г. – 30,4%; над 4 г. – 34,1%, като и според общия трудов стаж: до 5 г. – 31,6%, до 15 г. – 31,7%; над 15 г. – 36,7%. В зависимост от броя на членовете в групата: под 10 човека – 49,8%, над 10 човека – 50,2%. Според образованието бакалаврите са най-голяма част от респондентите (59,2 %) и са почти два пъти повече от магистрите (30,8%) и пет пъти повече от служителите със средно образование (10,0%). В научно-изследователските колективи: нехабилитирани – 70,4 %, хабилитирани – 29,6 %.

За да се установи влиянието на типовете организационна култура върху видовете конфликти и стратегиите за разрешаването им, е направен **регресионен ана-**

лиз по метода на множествената стъпкова регресия, като от значение са данните на първата стъпка. Измерва се липсата на определената променлива в ситуациите на взаимовлияние. Коефициентът на регресията (Standardized Coefficients) е β. Представени са данни за стандартизираните и нестандартизираните β-коефициенти на променливите и за степента на значимост. Въз основата на стандартизираните β-коефициенти е възможно директно сравняване и преценка на относителната тежест на всяка променлива. Тъй като се използват няколко зависими променливи, се въвежда като допълнителен коефициент ΔR^2 — Adjusted R Square за процента на обяснената вариация.

Издигнатите хипотези се потвърдиха до голяма степен. Данните от направения регресионен анализ отчитат влияние на всеки един от типовете организационна култура върху видовете конфликти (вж.Табл. 1) и стратегиите за разрешаването им (вж.Табл. 2). Изключение прави отстъпчивата стратегия за всеки един от изследваните сектори на дейност. Това поставя под въпрос очакванията на хората да разрешават проблема на практика, макар че се стимулира сътрудничество. По скоро се търси възможност да се получи нещо в замяна, при положение, че ситуацията е усложнена и задълбочена.

Табл. 1. Влияние на типовете организационна култура върху видовете конфликти

Орг.култура / *Конфликти*	*Правила*	*Иновации*	*Цели*	*Подкрепа*
Междугрупов			За изд. β = -336*; ΔR^2 = 0.089	За МА β = -0.367**; ΔR^2 = 0.357
Вътрешно-групов	За НИД β = 0.267*, ΔR^2 = 0.07	За ИТ β =-0.138*, ΔR^2 = 0.50	За МА β = -0.089*; ΔR^2 = 0.006 За ИТ β = -0.238*; ΔR^2 = 0.50	За МА β = -0.412**; ΔR^2 = 0.408
Ролеви		За търг. β = -0.246*, ΔR^2 = 0.15	За МА β = 0.517**; ΔR^2 = 0.06	За МА β = -0.520***; ΔR^2 = 0.260

****p < 0.001; **p < 0.01; *p <0.05*

Степента, в която се изразяват типовете ценностни предпочитания успява да разкрие, че организационните конфликти и стратегии за разрешаването им са в състояние да изградят стабилна мотивация и привързаност към работната среда. Най-вече подобна констатация е валидна за сферите на дейност, свързани с мехатрониката и автоматизацията, където културата на подкрепата влияе положително както върху междугруповите (β = -0.367**; ΔR^2 = 0.357), така и върху вътрешногруповите (β = -0.412**; ΔR^2 = 0.408) и ролевите конфликти (β = -0.520***; ΔR^2 = 0.260). Трябва да се уточни, че отрицателните стойности показват не наличието, а липсата на конфликти, според използвания инструментариум. По принцип придържането към нормите на подкрепа и следване на организационните цели в МА (β = -0.089*; ΔR^2 = 0.006) и ИТ (β = -0.238*; ΔR^2 = 0.50) са основата за формиране на доминиращите ценностни предпочитания. Ориентацията към запазване на стабил-

ността на системата важи с пълна сила и за сферата на издателската работа, особено при междугруповите конфликти (β = -336*; ΔR^2 = 0.089). Когато ролевите конфликти са овладяни или са в ниска степен, то тогава нараства личната заинтересованост и предприемчивост в сферата на търговията (β = -0.246*, ΔR^2 = 0.15). Междуличностните противоречия не са в услуга на никого, особено за подкрепа на иновациите и предприемането на премерени рискове според респондентите в ИТ (β = -0.138*, ΔR^2 = 0.50). За хората от НИД вътрешногруповите конфликти не влияят добре на дисциплината и спазването на нормите при съвместната работа, в противоречие са с писаните и неписаните правила и стандарти, а съобразяването с груповите закони улеснява междуличностната комуникация и социализацията на нови членове в групата.

Доминиращите ценностни предпочитания към подкрепата влияят положително върху всяка стратегия за разрешаване на конфликти при МА и НИД. Продължителните конфликти се смята, че са нежелателни за каквито и да било ситуации: за внедряването на иновации (β = 0.308*; ΔR^2 = 0.10), за постигането организационните цели (β = -0.469**; ΔR^2 = 0.233) и за междуличностната толерантност (за МА β = -0.339***; ΔR^2 = 0.408; за библ. – β = -0.213*; ΔR^2 = 0.36).

Табл. 2. Влияние на типовете организационна култура върху стратегиите за разрешаване на конфликти

Орг.култура / Стратегии	*Правила*	*Иновации*	*Цели*	*Подкрепа*
Интегрираща		За МА β = 0.308*; ΔR^2 0.10	За НИД β=-0.469**; ΔR^2=0.233	За МА β = -0.339***; ΔR^2 = 0.408 За библ. - β = -0.213*; ΔR^2 = 0.36
Избягваща		За търг. β = -0.138*, ΔR^2 = 0.30	За МА β =-0.233*; ΔR^2 = 0.12	За МА β = -0.461**; ΔR^2 = 0.21
Доминираща				За МА β = -0.237**; ΔR^2 = 0.452
Компромисна	За НИД β = 0.288*; ΔR^2 = 0.07	За МА β = 0.375**; ΔR^2 = 0.134 За НИД β = 0.357**; ΔR^2 = 0.114	За НИД β = 0.252*; ΔR^2 = 0.05	За НИД β = 0.394**; ΔR^2 = 0.143

****p < 0.001; **p < 0.01; *p <0.05*

Най-ефективни форми за промяна на конфликтната ситуация се смята, че са онези, които позволяват да се реши конфликта чрез компромис, независимо дали става въпрос за отказ от нещо ценно в името на груповата цялост (за НИД β = 0.288*; ΔR^2 = 0.07) или в името на творческия напредък (за МА β = 0.375**; ΔR^2 = 0.134; за НИД β = 0.357**; ΔR^2 = 0.114), или заради общите цели (за НИД β = 0.252*; ΔR^2 = 0.05) и взаимната подкрепа (за НИД β = 0.394**; ΔR^2 = 0.143). Прео-

доляването на проблема се корени в намирането на причината довела до конфликта. Може да се твърди, че се стимулира положително отношение. Начинът, по който се търси разрешаване на конфликта до голяма степен се ръководи от поведението в самата конфликтна ситуация и от съобразяването с йерархичните позиции (за МА β = -0.237**; ΔR^2 = 0.452). Пасивното оттегляне от ситуацията се прилага тогава, когато вредите от евентуалната конфронтация биха надхвърлили ползата от разрешаването на конфликта и е предпочитан при въвеждане на нови методи на работа (за търг. В = -0.138*, ΔR^2 = 0.30) или е естествена реакция в трудни ситуации (за МА β = -0.233*; ΔR^2 = 0.12), но той е временно решение и не е подходящ при важни проблеми, чието отлагане би влошило още повече конфликта (за МА β = -0.461**; ΔR^2 = 0.21). В случаите, когато конфликтът е продиктуван от самия предмет на съвместната дейност, той може да изпълнява и позитивна функция. Конфликтите са необходим елемент на движението. Ценността на конфликта се състои в това да предпазва социалната система от закостенялост и открива пътя на иновациите. Конфликтите са важен елемент на социалното взаимодействие, който способства за разрушаване или укрепване на определени социални връзки.

Изводи

Доминиращите ценностни предпочитания допринасят пряко за поддържане на сигурността и за справянето с кризите и конфликтите в организациите. Потвърди се издигната хипотеза за високи стойности на влияние на типовете организационна култура върху видовете конфликти и стратегиите за разрешаването им в различните сфери на дейност. Залага на вътрешната стабилност и интеграция на работното място.

Културата на целите и културата на правилата в по-голяма степен определят проявите на подчинение и участие и в по-малка на алтруизъм и съгласие. Това има значение както за изграждането на кооперирането, координацията и екипната работа като критични фактори за успех, така и за въвеждане на промяна и иновации в работата.

Въз основа на проведеното изследване в различни сфери на дейност се установи, че доминиращите ценностни ориентации варират според сферите на дейност. Разкрива се тенденция за усвояване на ценностите на работа, ориентирани към постигане на добри резултати, проактивно поведение, поемане на отговорност, новаторство.

Според резултатите от регресионния анализ най-силно влияние се отчита при културата на подкрепата при всички видове конфликти и стратегии за разрешаването им в сферата на мехатрониката и автоматизацията и информационните технологии. Установи се, че компромисната стратегия за справяне с проблемните ситуации е предпочитана предимно в сферата на научноизследователската дейност. В сектора на търговията културата на иновациите повлиява избягващата стратегия и спазаването на неутралност при кризи и конфликти. В издателската и библиотечните сфери се извеждат тенденции за осъзнати и целенасочени прояви на оказване на помощ на колеги, пряма дискусия, защита на организационните интереси, както и отстъпление от междугруповите конфликти. Те могат да бъдат обвързани, както с динамичните промени във външната среда, така и с постигането на контрол върху изпълнението. Резултатите от регресионния анализ показват, че културата на подкрепата и културата на иновациите най-силно детерминират стратегиите за разрешаване на конфликти. Това предполага висока степен на отговорност и включеност

в организационните процеси и стремеж към дискусия за намиране на креативни подходи при разрешаването на възникналите конфликтни ситуации.

Данните от настоящия анализ могат да се приложат от една страна за повишаване общата комуникативна компетентност, а от друга – да се поддържат доминиращите ценностни предпочитания, които биха повлияли за избор на най-добра стратегия за разрешаване на кризите и конфликтите в организацията.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. De Witte, K., Van Muijen, Koopman, P., De Cock, G., at al. The FOCUS-instrument for measuring organizational climat and culture in nine euronean languages. 14th Newsletter of the International Research Group FOCUS, 1996
2. Rahim, M. A. (1997). Styles of managing organizational conflict: A critical review and synthesis of theory and research. In M. A. Rahim, R. T. Golembiewski, & L. E. Pate (Eds.), *Current topics in management* (Vol. 2, pp. 61–77). Greenwich, CT: JAI Press.
3. Илиева, С. Организацинна култура. - София: Унив.изд. Св. Кл. Охридски, 2006, 332с. ISBN – 10: 954-07-2480-5
4. Карабельова, С. Управление и развитие на човешкия потенциал. – София : Класика стил, 2004. ISBN – 954-9964-95-7
5. Rahim, M. A.. (1983a). Measurement of organizational conflict. *Journal of General Psychology, 109,* 189–199.
6. Rahim, M. A. (1983b). A measure of styles of handling interpersonal conflict. *Academy of Management Journal, 26,* 368–376.
7. Илиева, С. Ценности и трудова мотивация– София: Унив.изд. Св. Кл. Охридски, 2011, 375с. ISBN – 978-954-07-2964-0
8. Карабельова, С. Ценностни и културни практики в България. – София : Класика стил, 2011, 343с. ISBN – 978- 954-357-074-3
9. Майяна Митевска-Енчева, Иновативни клъстери и организационна култура, София, За буквите 2012, 156 с. ISBN 978-954-2946-46-5
10. Фролов, С. Социология организаций. Организационные конфликты. Общее представление о конфликтах в организации. (May 2014) http://society.polbu.ru/frolov_esociology/ch34_i.html
11. Armstrong, M. Personnel Management Practice. Kogan Page, 1991
12. Deal, T., Kennedy, A. Corporate culturees: The rules and rituals of corporate life. Reading, MA: Adison – Wesley, 1982.
13. Rahim, M. A. (1980). Some contingencies affecting interpersonal conflict in academia: A multivariate study. *Management International Review, 20* (2), 117–121.
14. Rahim, M. A. (1979). The management of intraorganizational conflicts: A laboratory study with organization design. *Management International Review, 19* (1), 97–106.
15. Rahim, M. A. (1980). Some contingencies affecting interpersonal conflict in academia: A multivariate study. *Management International Review, 20* (2), 117–121.
16. Rahim, M. A. (1983c). *Rahim Organizational Conflict Inventory–I.* Palo Alto, CA: Consulting Psychologists Press.
17. Rahim, M. A. (1983d). *Rahim Organizational Conflict Inventory–II, Forms A, B, & C.* Palo Alto, CA: Consulting Psychologists Press.
18. Rahim, M. A. (1983e). *Rahim organizational conflict inventories: Professional manual.* Palo Alto, CA: Consulting Psychologists Press.

19. Rahim, M. A. (1986). Referent role and styles of handling interpersonal conflict. *Journal of Social Psychology, 126,* 79–86.
20. Schein's, Edgar H. Model of Organizational Culture. (May 2013) <http:((www.valuebasedmanagement.net(methods_schein_three_levels_culture.html>.
21. Schein, E. Organizational Psychology. NJ, Prentice Hall, 1980, pp. 34-67 ISBN 0-13-641332-3, (May 2013)

ЕФЕКТИ НА ОРГАНИЗАЦИОННИ ЦЕННОСТИ ВЪРХУ ПРОЯВИТЕ НА ПРОСОЦИАЛНОТО ПОВЕДЕНИЕ

Майяна Митевска-Енчева

Университет по библиотекознание и информационни технологии, София

EFFECTS OF VALUE SIGNS ON MANIFESTATIONS OF PRO-SOCIAL BEHAVIOUR IN ORGANIZATIONS

Mayiana Mitevska-Encheva

***ABSTRACT**: The research records the specifics of pro-social behavior in organizations. The effects of value signs on the choice of helping behavior have been analyzed. Data have been processed with SPSS-16. The results of the research could serve for the development of social and communication skills in the organization.*

***KEY WORDS**: pro-social behavior in organizations*

Увод

Просоциалното поведение се приема като положително и алтруистично поведение, което „надскача конкретните изисквания на работата ... и подпомага благополучието на работната група и организацията“ [1]. То се описва като благоприятно за организацията поведение, включващо също така предпазване на организацията от неочаквани опасности и сътресения, положителни изказвания за живота в организацията пред външни лица, поддържане на нейния добър имидж и т.н. Освен, че просоциалното поведение се състои от реакции, които носят облаги единствено на реципиента, то се детерминира от вътрешни и външни механизми. Първите се усвояват и направляват от общите принципи на морала, при външните ударението е върху социалната среда и ситуация.

Организационните ценности се изразяват до голяма степен в определенията на организационната култура и климат. Изследва се и влиянието на типовете конфликти и стратегиите за разрешаването им като показател за състоянието на организационните ценности.

В обобщен вариант културата характеризира реалното положение на нещата в организацията, а климатът – усещането на хората за положението на нещата. Следователно, при обща организационна култура, климатът в различните отдели може

да бъде контрапункт на приетите правила и норми. Анализът на климата е насочен към изследване мненията на хората и реакциите им на определени ситуации. Или климатът, това е начинът, по който служителите възприемат културата на организацията, начинът, по който я виждат те и начинът, по който я чувстват [2].

Макар че описват комплекс от характеристики на една организация, организационните конфликти и стратегиите за разрешаването им се приемат за две отделни по тежест понятия. Обобщено може да се приеме, че конфликтът е нормална проява на социалните връзки и отношения между хората, начин на взаимоотношение при несъвместими ценности, сблъсък на интереси, противоборство на парадоксално взаимосвързани от общи допирни точки страни. При стратегиите за разрешаване на конфликти се отчита спецификата на конкретната ситуация, участниците в нея и сложността на проблема като детерминанти, съпътстващи всеки конфликт.

Организационната култура, климат, типове конфликти и стратегии за разрешаването им позволяват да бъдат адекватно измерени и да се отчете влиянието им върху проявите на просоциалното поведение. Основанията за това са, че те са най-силните и предиктивни фактори, които ясно могат да определят ефектите на организационните ценности.

Предполага се, че просоциалното поведение, което се характеризира с „инициативност и доброволно ангажиране с дейностите в организацията“ [3] изпълнява определена роля, върху която оказват влияние различни фактори.

Хипотезата е, че различните типове организационна култура и климат, както и типовете организационни конфликти и стратегиите за разрешаването им влияят значимо върху различни прояви на просоциално поведение.

Методи

Използван е Въпросникът за просоциално поведение на Ван Дюн и колеги (Van Dyne, Graham, Dienesch, 1994), адаптиран за българските условия от С. Илиева [3]. Тази методика е съставена от 48 твърдения с пет подскали, характеризиращи различните прояви на просоциалното поведение като многодименсионален конструкт: *лоялност, подчинение и участие, алтруизмът, съгласие.* Скалите са свободни от социална желателност. Надеждността на въпросника е висока (α=0.74). Отделните подскали показват добра надеждност според коефициента α на Кронбах. С тази методика може да се изследва и евентуалната промяна на просоциалното поведение и да се открият тенденции в развитието им, свързани с динамичните промени във външната среда.

За отчитане на влиянието на организационната култура и климат се използва въпросника ФОКУС [3]. Той съдържа две самостоятелни части. Конструктите се вписват в четири основни ценностни ориентации към: *целите, подкрепата, иновациите и правилата*. Измеренията на организационната култура се конструират в 35 твърдения, където се оценява колко типични за организацията според изследваните лица са те. Използва се шестстепенната скала на Ликърт, която варира от „никога“ до „винаги“. Надеждността на въпросника е висока (α=0.86) и с добра надеждност според коефициента α на Кронбах (С. Илиева, С. Карабельова) [6, 11].

Параметрите за измерване на организационния климат обособяват 40 твърдения. Оценяват се по шестстепенна скала като се дава отговор на въпросите „Колко хора?“ и „Колко често?“ като зададеният формат за отговори е съответно от „никой“ до „почти всички“ и от „никога“ до „почти винаги“. Въпросникът „ФОКУС“ е адаптиран за българските условия от С. Илиева и показва високи психометрични

качества - α на Кронбах е 0.93. Измерват се четири типа организационен климат: цели, подкрепа, иновации и правила, които отразяват съответните ценностни практики в организацията.

Използвани са и методики за изследване на състоянието на конфликтите в организацията, както и стратегиите за тяхното разрешаване. Основанието за това е, че конфликтите в организацията и изборът на стратегия за разрешаването им са ясен индикатор за доминиращите ценности в организационна среда. Методиките за типовете конфликти в организацията и стратегиите за разрешаването им са разработени под ръководството на Рахим Афзал [5]. Типовете конфликти са разделени на три вида: междугрупов, вътрешногрупов и ролеви. Съставена е от 21 твърдения, които разкриват съответно наличието или липсата на конфликти. За всеки тип конфликт са зададени по 7 твърдения като между тях има и реверсивни. Оценките се дават по 5-степенна скала на Ликърт, започвайки от 1 – напълно не съм съгласен до 5 – напълно съм съгласен. Надеждността на въпросника е много висока (α=0.89). Отделните подскали показват добра надеждност според коефициента α на Кронбах.

Въпросникът за стратегиите за разрешаване на конфликти [6], разглежда пет стила описващи интегриращия, избягващия, доминиращия, услужливия и компромисния стил и се състои от 35 твърдения.

Чрез използването на статистически програми се очаква да се изведат онези променливи, които имат най-силен ефект върху организационните ценности. За целта се използва *регресионен анализ.* Той разглежда изучаваните процеси като зависими от един или повече фактори, които в различна степен влияят върху тяхното протичане. Въведени са две случайни променливи, между стойностите на които съществува линейна зависимост. Бета (β) е параметърът на линейното уравнение и се нарича регресионен коефициент. Бета (β) измерва изменението, което настъпва в явлението-следствие на явлението-фактор с цел да се изявят причинно-следствените връзки и съответните зависимости. В изследването е използван методът на множествената стъпкова регресия. От значение са данните на първата стъпка. Измерва се липсата на определената променлива в ситуациите на взаимовлияние. Представени са данни за стандартизираните и нестандартизираните β-коефициенти на променливите и за степента на значимост. Въз основата на стандартизираните β-коефициенти е възможно директно сравняване и преценка на относителната тежест на всяка променлива. Тъй като се използват няколко зависими променливи, се въвежда като допълнителен коефициент ΔR^2 — Adjusted R Square. Той показва процента на обяснената вариация. С цел да се провери хипотезата за прогностичната функция на организационния климат върху проявите на просоциалното поведение, е проведен стъпков регресионен анализ. Статистическият процес, чрез който може да се осъществи проверката на тази хипотеза, предполага конструирането на регресионно уравнение със зависима променлива „просоциално поведение“ и независими променливи „типове организационна култура“, „типове организационен климат“, „типове конфликти в организацията“, „стратегии за разрешаването на организационните конфликти“.

Данните са обработени със стандартния пакет статистически програми SPSS-16.

Извадка. Изследвани са 623 човека в период 2011г. - 2012г. Респондентите са разпределени по групи, в зависимост от изследваните демографски признаци. Жените (63,3%) са приблизително два пъти повече от мъжете (36,7%). В зависи-

мост от заеманата позиция в организацията мениджърите са 15,8%, а изпълнителите – 84,2%. Според стажа в конкретна организация респондентите са разпределени в три групи: до 2 години – 35,5%, до 4 години – 30,4%; над 4 години – 34,1%, както и според общия трудов стаж: до 5 години – 31,6%, до 15 години – 31,7%; над 15 години – 36,7%. В зависимост от броя на членовете в групата: под 10 човека – 49,8%, над 10 човека – 50,2%. Според образованието бакалаврите са най-голяма част от респондентите (59,2 %) и са почти два пъти повече от магистрите (30,8%) и пет пъти повече от служителите със средно образование (10,0%).

Хипотезата за значимо влияние на организационните ценности върху проявите на посоциалното поведение не се потвърди. Данните от направения регресионен анализ (Табл.1) отчитат влияние единствено на културата на целите върху проявите на подчинение на просоциалното поведение ($\beta = 0.078$, $p<0.05$).

Табл. 1. Влияние на видовете организационна култура върху проявите на организационно гражданско поведение

Орг. култура / Просоц. повед.	Култура на правила	Култура на иновации	Култура на цели	Култура на подкрепа	ΔR^2
Подчинение			$\beta = 0.78$, $p<0.05$		0,36

Проявите на спазването на нарежданията, зададените указания и заповеди логично се влияе положително, макар и слабо от организационните ценности, свързани с контрола и спазването на нормите на работното място. Подчертава се законността, легитимността и отговорността, както и изключителното значение на йерархията и статуса в организацията. Ценностите са свързани с доброто изпълнение, отговорността, измерването на изпълнението. Подобно въздействие се смята за съществено, тъй като задава 36% от вариацията. Фокусът е насочен върху изпълнението на задачите и лидерските качества се основава на подходящото знание и компетентност.

Резултатите от изследването не отчетоха влияние на нито един от типовете организационен климат върху проявите на просоциалното поведение. Степента на идентификация с организацията и възможността за професионална реализация в нейните граници са незначителни и не разкриват ясно кой от типовете организационен климат е в състояние да изгради у тях стабилна мотивация, привързаност към работната среда и прояви на подпомагащо поведение.

Данните от регресионния анализ не отчитат влияние на нито един от типовете организационни конфликти върху проявите на просоциалното поведение.

Единствено доминиращата стратегия за разрешаване на организационни конфликти (Табл. 2.) влияе слабо върху лоялността към организацията ($\beta = 0.089$, $p<0.05$), с 8% от вариацията.

Табл. 2. Влияние на стратегиите за разрешаване на конфликти върху проявите на организационно гражданско поведение.

Стратегии / Просоц. повед.	Интегр.	Избяг.	Домин.	Услуж.	Компром.	ΔR^2
Лоялност			$\beta = 0.89$, $p<0.05$			00.008

Проявите на лоялност се влияят доминиращата стратегия за разрешаване на конфликти. Тя е приемлива при въвеждането на непопулярни мерки или новости в организацията и напълно подходящ за колективи, в които социално-психологическия климат се характеризира с откритост, доверие и участие на екипа в процеса на вземане на решения. Допустимо е да бъде налаган и при много кратки срокове за изпълнение на задачата. Лоялността към организацията е детерминирана от търсенето на компромис, провокирано от страна на лидерите и е пресечната точка на постигане на съгласуваност, защото страните в конфликта получават умерено удовлетворение на потребностите и интересите си.

Изводи. Предположенията, че организационните променливи имат силна детерминираща роля върху просоциалното поведение не се потвърдиха. Регистрираните стойности са слаби или незначими. Данните от изследването отчитат единствено влиянието на културата, ориентирана към организационните ценностите на целите и доминиращата стратегия за разрешаване на конфликти като въздействащи съответно подчинението и лоялността в организацията. Следователно, изследваните организационни променливи детерминират слабо проявите на просоциалното поведение. В заключение може да се каже, че формирането на подпомагащо поведение се детерминира от ясно поставените цели в организацията и разрешаването на конфликтите с размах от позицията на авторитета и властта.

Данните от настоящия анализ могат да се използват за повишаване общата професионална комуникативност и идентифициране на проявите на подпомагащо поведение, които биха повишили устойчивостта на организацията в динамичната външна среда.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Organ, D. W. Organizational Citizenship behavior: The good soldier syndrome. Lexington, MA: Lexington Books, 1988, p. 8.
2. Джонев, С. Социална психология. Т. 5. София, Софи – Р, 2004, 316 с. ISBN – 954-638-127-6
3. Илиева, С. Организацинна култура. - София: Унив.изд. Св. Кл. Охридски, 2006, 332с. ISBN – 10: 954-07-2480-5
4. De Witte, K., Van Muijen, Koopman, P., De Cock, G., at al. The FOCUS-instrument for measuring organizational climat and culture in nine euronean languages. 14th Newsletter of the International Research Group FOCUS, 1996
5. Rahim, M. A. (1997). Styles of managing organizational conflict: A critical review and synthesis of theory and research. In M. A. Rahim, R. T. Golembiewski, & L. E. Pate (Eds.), Current topics in management (Vol. 2, pp. 61–77). Greenwich, CT: JAI Press.
6. Карабельова, С. Управление и развитие на човешкия потенциал. – София: Класика стил, 2004. ISBN – 954-9964-95-7
7. Rahim, M. A.. (1983a). Measurement of organizational conflict. Journal of General Psychology, 109, 189–199.
8. Rahim, M. A. (1983b). A measure of styles of handling interpersonal conflict. Academy of Management Journal, 26, 368–376.
9. Джонев, С. Стратегии на ръководителя в междуличностните отношения, София, Наука и изкуство, 1990, с.48-87.

10. Илиева, С. Привързаност към организацията. – София: Изд. Албатрос, 1998. с. 171-174.
11. Илиева, С. Организационно развитие: Второ преработено и допълнено издание. – София:Унив.изд. Св. Климент Охридски – 2006, 269с. ISBN – 13: 978-954-07-2321-1
12. Илиева, С. Ценности и трудова мотивация– София: Унив.изд. Св. Кл. Охридски, 2011, 375с. ISBN – 978-954-07-2964-0
13. Карабельова, С. Управление и развитие на човешкия потенциал. – София : Класика стил, 2004. ISBN – 954-9964-95-7
14. Карагяурова, Д. Просоциалното поведение като междуличностно отношение. – Варна: Стено, 2010, 246с. ISBN – 978-954-449-499-5
15. Корсини, Р. под ред. Енциклопедия по психология, С: Наука и изкуство, 1998. ISBN – 954-02-0210-8
16. Ригио, Роналд. Въведение в индустриалната/организационната психология. – София: Издателство Дилок, 2006. 550с. ISBN – 10: 954-9994-43-0
17. Мещерякова, Б.Г., под ред. Большой психологический словарь. — М.: Прайм-ЕВРОЗНАК., 2002
18. Майяна Митевска-Енчева, Просоциално поведение и организационен климат, София, За буквите 2013, 201 с. ISBN 978-954-2946-75-5
19. Чалдини, Р., Д. Кенрик, С. Нейберг Социальная психология, Пойми других, чтобы понять себя, Санкт Петербург прайм-Еврознак, Издательский дом Нева, Москва, Ольма пресс, 2002, 3-ое международное издание. ISBN – 5-93878-076-4
20. De Witte, K., Van Muijen, Koopman, P., De Cock, G., at al. The FOCUS-instrument for measuring organizational climat and culture in nine euronean languages. 14th Newsletter of the International Research Group FOCUS, 1996
21. Deal, T., Kennedy, A. Corporate culturees: The rules and rituals of corporate life. Reading, MA: Adison – Wesley, 1982.
22. Mayiana Mitevska-Encheva Psychological Research in the Field of Knowledge Managers and Workers in Bulgaria. International Jornal of Social Sciences, Prague, International Institute for Social and Economic Sciences. IISES Vol. II. 03/2013, pp. 93-104.
23. Mayiana Mitevska-Encheva Interdependence and Mutual Influence of Pro-social Behavior and Organizational Climate In Different Arias of Activity in Bulgaria. The Macrotheme Review 2(6), Special Issue: International Macro Themes, 2013, pp. 47-57.
24. Organ, D. W. Organizational Citizenship behavior: The good soldier syndrome. Lexington, MA: Lexington Books. 1988 p.8.
25. Reichers, A.E., B. Schneider. Climate and culture: An evolution of constructs. San Francisco,Jossey-Bass, 1990, p. 22.
26. Smith, C., Organ, D., Near, J. Organizational citizenship behavior: Its nature and Antecedents. Jornal of Appied Psychology, 68: 653-663, 1983
27. Schein's, Edgar H. Model of Organizational Culture. (May 2013) <http:((www.valuebasedmanagement.net(methods_schein_three_levels_culture.html>.
28. Schein, E. Organizational Psychology. NJ, Prentice Hall, 1980, pp. 34-67 ISBN 0-13-641332-3, (May 2013)

29. Van Dyne, L. Graham, J., Dienesch, R. Organizational citizenship behavior: Construct redefinition, measurement, and validation. Academy of Management Jornal, ISBN – 37:765-802. 1994

СПЕКУЛАТИВНА АТАКА СРЕЩУ ФИКСИРАНИЯ ВАЛУТЕН КУРС. РЕАЛНА ЗАПЛАХА ЗА ФИНАНСОВАТА СИГУРНОСТ НА Р. БЪЛГАРИЯ ПРИ СЪВРЕМЕННИТЕ УСЛОВИЯ

Станимир Ст. Станев

Университет по библиотекознание и информационни технологии. Институт за научни изследвания и обучение на докторанти (ИНИОД), гр. София

SPECULATIVE ATTACKS ON FIXED EXCHANGE RATE. REAL THREAT TO THE FINANCIAL SECURITY OF THE R. BULGARIA IN MODERN CONDITIONS

Stanimir St. Stanev

***ABSTRACT**: In the research I will discuss the speculative attack as a real threat to the financial security of the R.Bulgaria.*

***KEY WORDS**: speculative attack; financial security; real threat.*

Функционирането на всяка държава е динамичен процес в търсене на непрекъсната адаптация и равновесие между вътрешни и външни фактори. Отсъствието на такова равновесие, поражда опасност от реализиране на заплахите за националнага сигурност и появата на организационни, институционални, финансови и друг вид кризи.

Финансовата сигурност, следва да се отнесе към основните съставляващи на категорийния апарат на националната сигурност. Но ако проблемите на националната сигурност са широко изследвани и представени в специалната литература, то същото не може да се твърди за финансовата сигурност на държавата, особенно когато тя е в условията на паричен съвет. Именно структура на този вид финансовата система, показва уязвимости, които изискват предефиниране на заплахите от гледна точка на функциониране на валутния борд.

Заплахите за финансовата сигурност се свързват с възможността да се причинят сериозни щети на финансовата система или да не се реализират целите, поставени пред нея. Първия резултат от реализиране на заплахите за финансовата сигурност на държавата е настъпването на финансова криза. Финансовата криза от своя страна е значително разстройство на публичните финанси, което е придизвикано от различни фактори, както и в контекста на обща икономическа криза. Финансовите кризи могат да бъдат групирани в три категории: банкова, дългова и валутна криза. Валутна криза е рязко увеличение на противоречията в паричната сфера, проявено като резки колебания в обменните курсове, бързи и значителни по мащаб

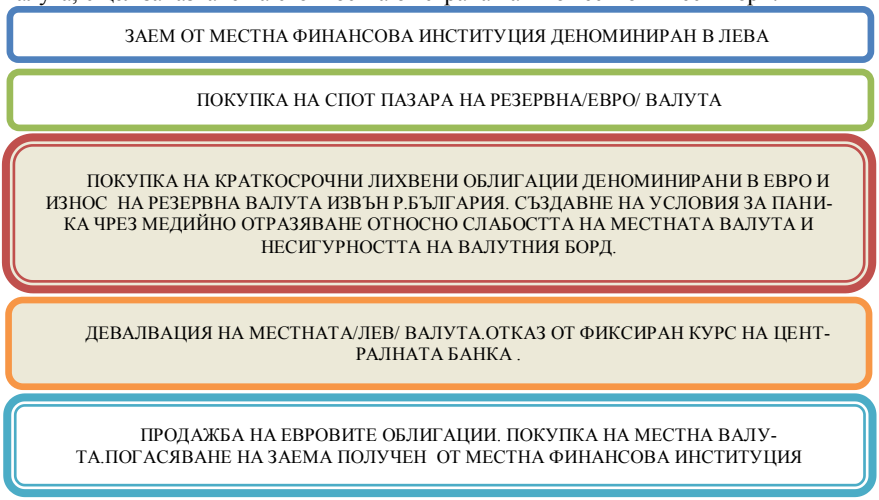
промени във валутните резерви на страната, девалвация и преоценка на валутния курс, влошаване на международната парична ликвидност.

Обект на интерес в това изследване е настъпването на валутна криза, чрез една от основните заплахи за финансовата сигурност на Р.България в условията на паричен съвет- спекулативна атака срещу фиксирания валутен курс.

За да се гарантира финансовата сигурност на Р.България в съвременни условия, е необходимо да се гарантира устойчивото функциониране на валутния борд. На база този показател, една от основните заплахи за финансовата сигурност е пряко корелирана с устойчивостта на валутния борд и се изразява в спекулативна атака срещу фиксирания валутен курс**.**

Спекулативна атака срещу фиксирания валутен курс, е чрез активни действия на пазарни участници/спекуланти/, да се застави Централната банка /ЦБ/ на страната, да изостави фиксирания валутен курс, като това е съчетано с масивни продажби на валутни активи. Очевидно е, че основната цел на валутните спекуланти е девалвиране на местната валута, като се изостави фиксирания курс и реализиране на печалба от възникналата курсова разлика. Всяка спекулативна атака е насочена към отслабване на националната валута в краткосрочен план, чрез значително увеличаване на предлагането и най-често се реализира от пазарен участник със значителни валутни активи. Негативните последствия от спекулативните атаки в краткосрочен хоризонт за икономиката са спад в цените на вътрешния пазар на ценни книжа, обезценяването на местната валута, повишаването на инфлационния натиск, и т.н.

Спекулативната атака е валутна операция, при която спекуланта разполага с достатъчно активи и счита, че съществуват достатъчно основания да се разклати доверието на пазара в атакуваната местна валута. При наличие на тези предпоставки, спекуланта трябва да вземе заеми в местната валута, да купи чуждестранна валута на местния пазар и да я изнесе извън страната /виж.фиг.1/. Това, комбинирано с достатъчна медийна подкрепа, ще доведе до масова продажба на местна валута, с цел запазване на стойността от страна на множество инвеститори.

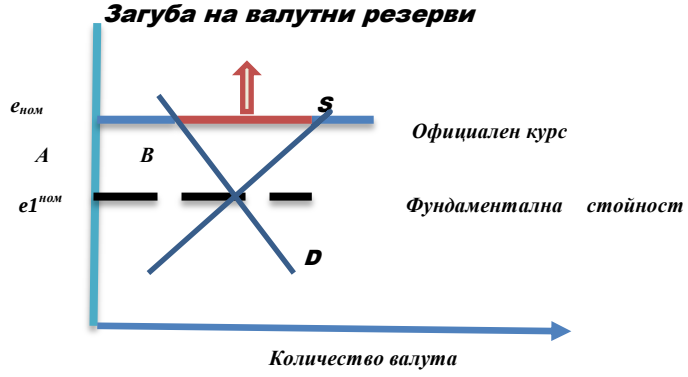


Фиг. 1. Етапи на протичане на спекулативна атака

Начинът, по който централната банка на страна с валутен борд може да реагира, е да продава валутните си резерви или да увеличи лихвените проценти до размер, при който икономическите агенти ще решат да инвестират отново в местната валута. Ако Централната банка не успее, ще трябва да изостави фиксирания курс, което е и целта на спекуланта. Проблемът с използването на валутните резерви е, че те са свързани с количеството местна валута в обръщение. Изтеглянето на местна валута от обръщение ще предизвика парализа на икономиката. Увеличаването на лихвените проценти ще се отрази на всички кредитополучатели и ще предизвика спад в икономическата активност, и ръст на безработицата. Затова, в някои случаи обезценяването на местната валута би било най-удачното и безболезнено решение. При положение, че местната валута се обезцени, спекуланта ще върне натрупаната валута в страната и ще купи местната обезценена валута с която да си върне заемите, като реализираната разлика ще бъде неговата печалба. Страните с функциониращи парични съвети, не са изложени често на такива атаки. Това е така, защото спекулантът трябва да разполага със огромни финансови възможности, да смята че владее пазара и да може да предизвика паника у икономическите агенти. Ако тези предпоставки са налице, шансовете за успех на спекулативната атака са големи.

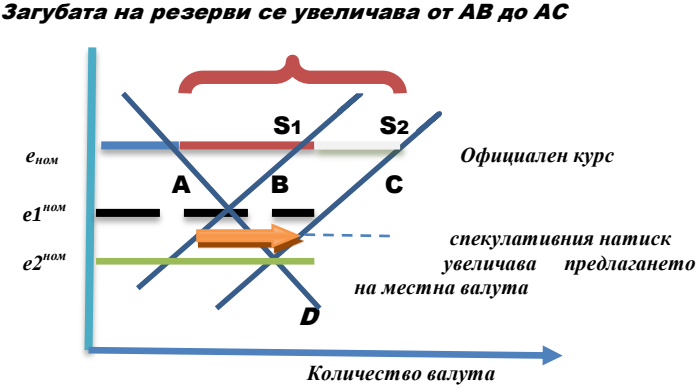
Един потенциален проблем със системата на фиксиран валутен курс е, че стойността на валутния курс определен от правителството-официален курс, може да не е същия обменен курс-фундаментална стойност, който се определя от търсенето **D** и предлагането **S** на валута. Фигура 2 показва ситуацията, когато обменния курс- **e**$_{\textbf{ном}}$ е по-висок от фундаменталната стойност на валутния курс.

Фигурата илюстрира положение, при което официално фиксирания номинален валутен курс със ставка **e**$_{\textbf{ном}}$, е по-висок от фундаменталната стойност на валутния курс **e 1**$_{\textbf{ном}}$, който се определя от пазарното търсене **D** и предлагане **S** на валутния пазар. Централната банка може да поддържа обменния курс на официално ниво, но за да стори това всеки път ще използва резервите си, за да купи от местния пазар валута в размер на **AB** . Тази загуба на резерви е известна още като дефицит на платежния баланс.



Фиг. 2. Загуба на валутни резерви

На база целенасочена спекулативна атака по фиксирания валутен курс и опита на Централната банка да поддържа нивото му на регламентираната му стойност, ще започнат масови продажби на местна валута поради страх от девалвация, което още по-вече ще увеличи натиск на местната валута и Централната банка ще бъде принудена да осигури предлагане на чужда валута в размер на **S2**. Това още по-силно ще амортизира валутните и резерви и ще увеличи загубата, от размер на **AB** до **AC**, и в даден момент тя ще се принуди да изостави поддържането на фиксиран валутен курс, което ще доведе до девалвация на местната валута.



Фиг. 3. Спекулативен натиск върху фиксирания валутен курс

До скоро в научната литература се е считало, че спекулативните атаки срещу фиксиран валутен курс, не могат да се случат в страни с валутен борд. Тъй като атаката предполага, че инвеститорите възприемат вероятността от девалвация с висока степен на вероятност, паричните власти на тези страни трябва да намалят предлагането на пари и увеличат драстично вътрешните лихвени проценти. Това огромно увеличение на лихвените проценти задължително ще доведе до тежка рецесия и безработица, което неминуемо ще срути брутния вътрешен продукт на страната и масово обедняване на населението.

За разлика от другите заплахи за финансовата сигурност на страната, които предимно са в резултат от прилагането на различни политики в държавното управление и функционирането на държавните органи, то спекулативната атака е активно целенасочено действие на субект или група от субекти, които целят постигането на конкретни политически или икономически резултати. Това поставя спекулативната атака срещу фиксирания курс в различен ракурс от другите заплахи за финансовата сигурност. Идентифицирането и неутрализирането на този вид заплаха изисква коренно различен подход и механизъм на взаимодействие между държавните органи и структури.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Неновски Н., К. Христов, Банковата система в условията на паричен съвет, ИПИ, С., 1999.
2. Неновски Н., К. Христов и Б. Петров (1999), "Два подхода към кризите на фиксираните курсове", БНБ, Дискусионни материали, бр. 4.
3. Неновски Н. (1997), "Теоретични основи на системните финансови кризи", сп. Икономическа мисъл, бр. 2, стр. 3 – 21..
4. Манчев Цв. (2001), "Финансови кризи и преструктуриране на финансовата система – теория, национална и международна практика", докторска дисертация, Софийски университет "Свети Климент Охридски", София.
5. Frankel, J., A. Rose, Currency Crashes in Emerging Markets: An Empirical Treatment. Journal of International Economics 41/1996.
6. Mishkin, F., Understanding Financial Crises: A Developing Country Perespective, NBER WP 5600 / 1997.

ФИНАНСОВА СИГУРНОСТ НА ДЪРЖАВАТА - ПОДСИСТЕМА НА СИСТЕМАТА ЗА НАЦИОНАЛНА СИГУРНОСТ

Станимир Ст. Станев

Университет по библиотекознание и информационни технологии. Институт за научни изследвания и обучение на докторанти (ИНИОД), гр. София

FINANCIAL SECURITY - SUBSYSTEM ON NATIONAL SECURITY SYSTEM

Stanimir St. Stanev

***ABSTRACT**: In the research I will discuss the place on financial security on national security system.*

***KEY WORDS**: financial security; national security.*

Сигурността е една от основните нужди на човека, обществото, държавата и човечеството. Нейната същност може да бъде описана, като способността да се отразява, предотвратява и отстранява опасностите, застрашаващи съществуването на посочените по-горе субекти, както и задоволяването на техните основни потребности, без удовлетворяването на които, би бил немислим животът, благополучието, развитието и напредъкът.

Науката в съвременния етап е разкрила, че много системи, включително и социалните, фактически разкриват тенденция към равновесие – в противен случай светът отдавна би се разрушил или би експлоадирал[8]. Равновесното състояние зависи от отношенията вътре в системата и от отношенията на системата с външния свят. Неопределеността, несигурността и случайността не са въпроси на нашето незнание, което може да се превъзмогне, а на самата изучавана реалност.

В теорията на изучаването на сигурността за разлика от икономиката и други научни направления, неравновесието и необратимостта се разглеждат като всеобхватен императив на обективната действителност. Изучаване на сигурността не отрича равновесните състояния, но не преминава през призмата на тяхната динамика. Изводът, който следва е, че именно неравновесието е източник на развитие и създаването на система с мощна отрицателна обратна връзка не може да бъде цел за управлението система свързана със сигурността.

Опасност, безопасност и риск се считат за основни (базови) концепции на теория на системите за сигурност. Най- общо понятието "сигурност" се възприема, като отразяване на вътрешни и външни заплахи насочени срещу сигурността на отделната личност, обществото и държавата. Разглеждайки така това понятие бихме могли да дефинираме нивата на сигурност и обектите, чиято сигурност би могла да бъде нарушена:

- Сигурност на Личността;
- Сигурност на Обществото;
- Сигурност на Държавата;

Националната сигурност обхваща нивата сигурност на личността, сигурност на обществото и сигурност на държавата, като цяло. Международната сигурност обхваща нивата сигурност на държавата, сигурност на общността от държави и сигурност на света.

В съвременен аспект националната сигурност се възприема като- защита на жизненно важните интереси на гражданите, обществото и държавата, на основата на която се гарантира непрекъснато развитие на обществото, ранно откриване, предотвратяване и неутрализиране на реални и потенциални заплахи за националните интереси.

Обекти на националната сигурност са:

• човекът и неговата индивидуалност/личност/ - конституционното му право и свободи;

•обществото - неговата духовна, морална, етична, културна, историческа, интелектуална и материална ценност, околната среда и природните ресурси ;

•държавата - конституционно установеният ред, суверенитета, териториалната цялост и неприкосновеност.

Финансовата сигурност е част от икономическата сигурност на държавата, която е основа на националната сигурност, и е определяща за другите видове сигурност- военната, политическата, икономическа и социална. Финансовата сигурност разполага със собствено съдържание, което я отличава от общите въпроси на икономическата сигурност. В литературата съществуват няколко дефиниции на понятието „финансова сигурност“, но най-близко до същността и би могло да се приеме, че финансовата сигурност на държавата е **съвкупност от условия и фактори, гарантиращи независимост, устойчивост и стабилност на финансовата система на държавата, включително поддържане на способност за постоянно развитие и самоусъвършенстване.** Създаването на този комплекс от минимално изискуеми условия, може да се постигне, като резултат от една целенасочена, ефикасна и ефективна управленска политика. На първо място, трябва да се обърне внимание на необходимостта да се направи разграничение между понятията "финансова сигурност на държавата", което е характерно за динамичното развитие на финансовата система, и "гарантиране на финансовата сигурност на държавата",

като съвкупност от организационни и правни отношения. Финансовата сигурност на държавата се основава на механизъм за гарантиране на финансовата сигурност на държавата, който е система от организационни, правни и институционални интервенции, насочени към своевременното откриване, предотвратяване, неутрализиране и отстраняване на заплахи за финансовата сигурност. Механизъм за гарантиране на финансовата сигурност на държавата, също така е единство на система от правни и други форми и методи, които осигуряват директен правен ефект, върху институциите на държавната власт в обществените отношения и в областта на финансите.

Очевидно е, че на базата на механизма за гарантиране на финансовата сигурност, се базира нормотворчеството и прилагане на законодателството, както и процесът на познание и оценка на правните потребности на обществото и държавата. Механизъм, който да гарантира финансова сигурност, може да се реализира чрез развитието на научните теории, концепции, стратегии и тактики на адекватна финансова политика, наличието на необходимите институции за сигурност, определянето и спецификацията на интереси, дефинирането и неутрализирането на заплахите застрашаващи финансовата сигурносст.

Като се има впредвид, че финансовата сигурност не е статична (на системата за сигурност се отразява конкретната ситуация, която се оформя в определен етап от социално-икономическото и политическото развитие на обществото), то механизмът на финансовата сигурност включва следните дейности:

- Обективен и всестранен мониторинг на икономиката и финансовия сектор, за да се идентифицират и прогнозират вътрешните и външни заплахи за финансовата сигурност;

- Изчисляване на *прагове*- критично допустимите стойности на финансово и социално-икономически показатели (индикатори), превишението на които може да предизвика финансова нестабилност и финансова криза;

- Дейности на държавата по отношение на откриване и предотвратяване на вътрешни и външни заплахи за финансовата сигурност.

Правната основа и концептуалните подходи по отношение на естеството на финансова сигурност, могат да определят, че обект на финансовата сигурност на държавата се явява финансовата система, и по-специално - всички нейни сфери и връзки като:

- човек, личност, домакинството;
- предприятия, институции и организации;
-отделни територии и региони;
-общество (неговите интелектуални и материални ценности, ресурси и др.);
- държава.

От практическа гледна точка, всички мерки насочени към осигуряване на финансовата сигурност следва да се съсредоточат върху конкретни обекти- човешки права и свободи, интереси и приоритети на граждански права, социални ценности, суверенитета и териториалната цялост на държавата.

Субекти за гарантиране на финансовата сигурност на държавата са Пезидент, Консултативен съвет за национална сигурност, Парламент, Съдебна власт, Правителство- министерствата и други централни органи на изпълнителната власт, Българска народна банка, ДАНС, Национална разузнавателна служба, МВР, КФН, Сметна палата, българските граждани и техните сдружения.

Цялостния концептуален подход към изследване на понятието-финансова сигурност, изисква да се очертаят приоритетите и националните интереси, по-големите заплахи за националните финансови интереси, и след това а се посочи механизмът за защита на финансовата сигурност на Р.България.

Приоритетни национални интереси във финансовия сектор са:

-Осигуряване на паричната и монетарната стабилност на обменния курс;

-Осигуряване на фискалната жизнеспособност на държавата;

-Укрепване на банковата система и увеличаване на националните спестявания;

-Укрепване на националния инвестиционнен капацитет и иновационната дейност на местни юридически лица;

-Реформа на финансовите пазари с цел да се гарантира независимостта на националната икономика, от международните флуктуации и колебания;

-Намаляване на влиянието на световната финансова криза върху финансовата система на Р.България;

Финансовата сигурност на държавата**,** е главното условие за способността на държавата да изпълнява своята собствена финансова и икономическа политика, в съответствие с националните си интереси.

Основните функции на системата за финансова сигурност:

-откриване и прогнозиране на вътрешни и външни заплахи за националните интереси, и обектите на финансовата сигурност на страната, прилагане на набор от оперативни и дългосрочни мерки за тяхното предотвратяване, и неутрализиране;

-създаване и поддържане на готовност на сили, и средства за гарантиране на финансовата сигурност на страната;

-управление на силите и средствата за осигуряване на финансова сигурност;

-определяне на границите и функционалните задължения на органите в системата на финансова сигурност;

Гарантиране на финансовата сигурност се основава на разделение на властите и правомощията на законодателната, изпълнителната, и съдебната власт .

Органите на изпълнителната власт**:**

- ✓ осигуряват изпълнението на законите и другите нормативни актове, регулиращи отношенията в сферата на финансово обезпечение;
- ✓ организират разработването и изпълнението на програми за национална и финансова сигурност;
- ✓ прилагат система от мерки за гарантиране на финансовата сигурност на личността, обществото и държавата, в рамките на своята компетентност;
- ✓ в съответствие със законодателството, създават, реорганизират или закриват органи на държавата за гарнтиране на финансовата сигурност.

Органите на съдебната власт:

- ✓ гарантират защита на конституционния ред в Република България, ръководейки се от Конституцията и законите на страната, правораздават в случаите на престъпления, които нарушават финансовата сигурност на личността, обществото и държавата;
- ✓ гарантират съдебната защита на гражданите, обществените и други организации и сдружения, чиито права са били нарушени, във връзка с дейностите за да се гарантира финансовата сигурност.

Основните елементи на финансовата сигурност са :

1. Бюджетна сигурност-под бюджетна сигурност трябва да се разбира, такова състояние на платежоспособност на държавата, съобразено с баланса на приходите и разходите на държавните и местните бюджети, и ефективност на бюджетните средства.

2. Данъчна сигурност-определя се от данъчната политика прилагана от изпълнителната власт, която най-оптимално обединява фискалните интереси на държавата, индивидуалните, и корпоративните интереси на данъкоплатците.

3. Сигурност по обслужване на външен и вътрешен/суверен/ дълг- изразява се в поддържането на определено ниво на вътрешен и външен държавен дълг, като се вземе предвид възможностите за неговото ефективно обслужване, и оптимален баланс, съчетавайки с реализиране на необходимите социално-икономическите потребности на обществото. Сигурността по обслужване на суверенния дълг трябва да е съчетана и със запазване стабилността на финансовата система от вътрешни и външни заплахи, като се гарантира относителна самостоятелност на държавата, и се поддържа адекватно ниво на платежоспособност, и кредитен рейтинг.

4. Валутна сигурност – изразява се в необходимия достатъчен обен на брутните валутни резерви за да се гарнтира фиксирания валутен курс.

5. Инфлационно-ценова сигурност и сигурност на паричното обращение-състояние на системите за разплащане и паричната система, които се характеризират със стабилност на паричната единица, достъпност до кредитни ресурси, и такива нива на инфлация, които обезпечават икономическия ръст, и повишават реалните доходи на населението.

6. Сигурност на банковата система и местните регулирани финансови пазари-гарантиране най-ефективно използване на ресурсния потенциал, създаване на благоприятни условия за финансовите интереси на банковите институции, превенция на вътрешни и външни заплахи за банковата система, създаването на условия за стабилно и ефективно функциониране.

Конструирането на финансовата сигурност на държавата е достатъчно сложен проблем, затова в процеса на формулирането на концепцията за финансова сигурност, трябва да бъдат изведени нейните най-съществени страни и аспекти на проявление, а самата финансова сигурност трябва да бъде представена като цялостна, единна и целенасочена система. Такъв подход би позволил не само ясно да се опише финансовата сигурност на страната, но и да послужи като методологична основа за анализиране на останалите равнища на проявление на финансовата сигурност.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Николай Слатински. Измерения на сигурността. Парадигма. С, 2000
2. Г. Стефанов. „Теория на международната сигурност“, Сиела, 2008г.
3. Дидык, В. Финансовая безопасность в системе экономической безопасности государства. В: Закон и жизнь, 2009.
4. Дидык В. Вопросы правового регулирования в области обеспечения финансовой безопасности США. В: Закон и жизнь, 2009.
5. Абалкин, Л. Экономическая безопасность России: угрозы и их отражение. В:Вопросы экономики. 1994.
6. Абдурахманов М. Основы национальной безопасности России. Под общей редакцией Манилова В.Л. М.: Друза. 1998.

7. Аксенов В. и др. Мировой финансовый кризис и экономическая безопасность России: анализ, проблемы и перспективы. М.: Экономика. 2010.
8. К. Боулдинг. Общая теория систем – скелет науки, с.116.

АСПЕКТИ НА СИГУРНОСТТА НА БАНКОВИТЕ ТРАНЗАКЦИИ, ОСЪЩЕСТВЯВАНИ ЧРЕЗ ПОС ТЕРМИНАЛ, ДЕБИТНИ И КРЕДИТНИ КАРТИ

Валентин Д. Стоянов, Христо А. Христов

Централна Кооперативна Банка, ШУ „Епископ Константин Преславски”

ASPECTS OF BANK TRANSACTION, SECURITY DONE THROUGH POS TERMINALS, DEBIT OR CREDIT CARDS

Valentin D. Stoyanov, Hristo A. Hristov

Central Cooperative Bank, Shumen University “Bishop Konstantin Preslavski”

***ABSTRACT**: Nowadays the development of economic life is marked with high stage of intensive globalization, heightened necessity for competitiveness and limitedness of such subjective resources like disposable time. One of the methods for saving in labour and time is the introduction of non-cash payment. Because of this it comes into question the security of performing operations.*

***KEY WORDS:**. EFT-POS, PIN code, TELEPHONE ORDER, MAIL ORDER, NO SHOW, PIN pad, cash advance, cashback/cashout, MasterCard VISA*

Съвременното развитие на икономическия живот, се характеризира с висока степен на интензивна глобализация, повишена необходимост от конкурентноспособност и ограниченост на такива субективни ресурси като разполагаемо време. Един от методите за пестене на труд и време е въвеждането на безкасовото плащане. Възниква въпросът за сигурността на извършваните операции.

Този въпрос може да се разглежда в два аспекта, защита на устройствата и защита на банковите карти.

Предимства на безкасовите разплащания пред касовите са свързани с гарантиране на сигурно, бързо и удобно разплащане, избягване на съществуващите недостатъци при касовите плащания, каквито са опасност от загубване на парите, грабеж и др.

Търговците, които приемат безконтактни плащания, също се възползват от предимствата на стандарта - повишена бързина на плащане, намаляване на опашките и увеличаване на оборота. Този тип картови разплащания е особено подходящ в търговски обекти с голям човекопоток и сравнително ниска стойност на едно плащане – вериги за бързо хранене, супермаркети, кафета, бензиностанции, кина, публичен транспорт, увеселителни паркове, паркинги и др. последните анализи на пазара показват, че използването на безконтактните плащания повишава с 30%

оборотите на търговците заради по-големия брой хора, които могат да бъдат обслужени в рамките на работния ден.

*ПОС терминала EFT-POS терминал**E**lectronic **F**unds **T**ransfer at **P**oint **O**f **S**ale* е устройство за приемане на директни плащания с дебитни и кредитни карти. ПОС терминално устройство работи в следната последователност:

- избира се желаната операция (покупка, покупка+пари в брой, преавторизация и други);

- въвеждат се данните за картата (номер, дата на валидност и секретен код);

- при поискване ПИН код POS терминалът се обръща към авторизационния център и при одобрение на операцията отпечатва разписка.

ПОС терминалите се подразделят на видове.

Според предназначението си ПОС терминалните устройства биват: Настолни - устройства, които са стационарни; Мобилни - преносими устройства с вградена батерия; За вграждане в други системи - устройства, които са част от по-голяма система.

Според вида на използваната връзка с авторизационния център ПОС терминалите биват: Dial-up - за връзка се използва обикновена кабелна телефонна линия; GPRS - използват SIM карта към мобилен оператор; Ethernet (LAN) - свързват се към интернет с кабел; Wi-Fi - свързват се към интернет чрез безжичен рутер/gateway; Bluetooth - използват Bluetooth gateway.

Видовете операции, които ПОС терминалите могат да изпълняват са:

- **Покупка** - най-типичната операция, при която търговецът получава от картата на клиента желаната сума;

- **Анулиране** на **покупка** - възстановяване на сума по картата на клиента;

- **Покупка на вноски** - (само при някои банки) разсрочване на покупка и удържане на първа вноска;

- **Авторизация** (позната още като Блокировка или Пре-авторизация). Операция, при която се извършва само блокировка на желаната сума, която в последствие може да бъде усвоена цялата или част от нея или да бъде освободена, деблокирана. Операцията е популярна в туристическия бизнес и отдаване под наем на автомобили (rent-a-car). Важна особеност на авторизацията е нейната валидност в случай, че не последва приключване или анулиране до няколко дни авторизацията се унищожава и сумата се деблокира, така че става достъпна за клиента. Валидността на авторизациите е различна в зависимост от политиката на банката, издател на картата (не от банката, чиито е ПОС терминала);

Приключване на авторизация - това е операция, при която блокираната сума чрез авторизацията се усвоява от търговеца. Приложима е основно в туристическия бизнес – например при резервация се блокира сумата а при напускане на хотела се усвоява блокираната сума за авторизацията;

- **Анулиране на авторизация** - освобождаване на блокирана сума;

- **Покупка** + **Пари в брой** - Един продукт на VISA, при който клиента има възможност при заплащане на покупка да изтегли и сума в брой от търговски обект;

- **Покупка** + **Бонус точки** - Натрупване на бонус точки при покупки на ПОС терминали свързани към лоялни програми;

Предплатен ваучер - (само при някои банки) Заплащане на ваучер с определен брой кредити;

- **Пари в брой** - операция, при която на клиента се изплаща сума в брой, взета от разполагаемия лимит на картата. Аналогична на изтегляне на пари от АТМ (банкомат). Операцията се изпълнява само в банка.

Въвеждане на данните за картата по няколко начина. Прочитане на картата чрез четеца на ПОС терминала е предпочитан начин за въвеждане на данните от гледна точка на сигурността и удобството. При повечето ПОС терминали това е единствения начин за въвеждане на данните за картата. Прочитането на картата през четеца на ПОС терминал се счита за по-сигурно, защото означава, че в момента на транзакцията картата е била налична, не се въвеждат на ръка откраднати данни. ПИН код (PIN code) При картитие с чип е нормално някои транзакции да не изискват ПИН код, а само подпис. Решението за това взима чип картата, съгласно политиката на банката издател. Преобладаващата част от картите имат магнитна ивица, която съдържа номера на картата, датата на валидност (понякога име на картодържателя). Тъй-като данните от магнитната ивица са лесно четими, освен това нямат надеждна защита срещу презапис, с напредването на технологиите постепенно се въведе интелигентен чип, който съдържа информация за картата, допълнителни данни и осигурява надеждна защита срещу прочитане и презапис. Картите от този тип са познати още като смарт карти или EMV карти на името на алианса от международни картови организации, които са разработили съвместно EMV стандарта за сигурност. Съвсем логично, транзакции с чип карта са по-надеждни от транзакции с карта, която има само магнитна ивица. Повечето ПОС терминални устройства разпознават наличие на чип и при прочитане на магнитната ивица на картата, изискват задължително прочитане на данните от чипа на картата.

Въвеждане на данните за картата от клавиатурата на ПОС терминала, този начин на въвеждане е познат, като key-entry. Приложението на този маниер на работа е при транзакции, при които в момента на транзакцията, картодържателят и картата не са при ПОС терминала. Използва се в следните случаи: резервация по телефона - "TELEPHONE ORDER"; резервация по имейл - "MAIL ORDER"; Глоба за неявяване по направена резервация - "NO SHOW".

В туристическия бизнес, при извършване на резервация клиентът предоставя данни за кредитна карта. Хотелите са длъжни да предвидят срок, в който клиентът има право да се откаже без такса от направената резервация. В случай, че клиентът не уведоми хотела в предвидения срок, но и не се яви на уговорената дата от резервацията, хотелът има право да направи "NO SHOW" транзакция, компенсация за пропуснатите ползи от неявяването на клиента.

Транзакциите с ръчно въвеждане на номера на картата са изключително рискови и се разрешават от банките след допълнително одобрение на търговеца.

При въвеждане на PIN (ПИН) код, трябва да се знае, че ПИН кода е личен секретен код, съставен обикновено от 4 цифри. Този код гарантира, че картата се използва от картодържателя. ПИН кодът обикновено се въвежда чрез специална външна специализирана клавиатура (PIN pad) или на самия ПОС терминал. Генерирането на първоначалния ПИН код при произвеждането на картата става в специални условия, при които полученото случайно число за ПИН код, се отпечатва върху лист, който е в запечатан плик. По този начин ПИН кодът е скрит, дори и за служителите, които участват в производството на карти.

Защита на ПИН кода се осъществява чрез:

• Ограничаване на броя грешно въведени ПИН кодове. Това е защита срещу опити за откриване на ПИН кода. В повечето случаи след третия грешен опит картата се блокира. В този случай само банката издател може да деблокира картата. Повечето банки издават и нов ПИН код;

• Криптиране на ПИН кода. При предаване на данните за транзакцията към авторизационния център информацията е криптирана;

• Сертификация за сигурност на устройствата за въвеждане на ПИН код. Платежната индустрия разработва и развива стандарти за сигурност. PCI PED стандартът гарантира сигурността на устройствата за въвеждане на ПИН кодове.

За осигуряване на сигурността при използване на банковата карта е необходимо да се знае, че тя е електронен платежен инструмент и представлява пластмасова карта, върху която е записана информация по електронен начин и която се използва многократно за идентификация на картодържателя, отдалечен достъп до банкова сметка и за извършване на следните операции:

• теглене на пари в брой чрез терминални устройства АТМ;

• плащане на стоки и услуги и получаване на пари в брой чрез терминални устройства ПОС;

• плащане на стоки и услуги чрез виртуални терминални устройства ПОС;

• превод между сметки чрез терминални устройства АТМ;

• плащане на услуги чрез терминални устройства АТМ;

• справочни и други платежни и неплатежни операции.

Основни характеристики на банковите карти са:

• Банкова карта може да се издаде само на физическо лице (картодържател).

• Банковата карта може да се използва само лично от картодържателя.

• Банкова карта се издава въз основа на договор за банкова карта, в който трябва да са указани правата, задълженията и отговорностите на банката-издател и картодържателя.

• Банковата карта е собственост на издателя. Издатели на банкови карти у нас са всички банки, които имат в издадената им от Българска народна банка лицензия за банкова дейност издаване и управление на банкови карти.

• Банкова карта е карта, която картодържателят може да използва, а търговецът да приема за плащане на покупка, услуга или погасяване на дълг.

На пазара са разпространени различни типове карти, но те притежават няколко общи признака. Изработени са от пластмаса с размери 85.60 × 53.98 mm, според стандарта ISO/IEC 7810 ID-1. Върху тях са гравирани обикновено името на картодържателя и банков номер според стандарта ISO/IEC 7812.

Обикновено банковата карта е свързана с банкова сметка, принадлежаща на картодържателя. Тази сметка може да е от най-различен вид. Например най-популярни са следните банкови карти:

• кредитна:

При тази карта издателят (финансовата институция) е създал предварително кредитна линия за клиента си картодържател, от която той може да тегли (т.е. да заема), за да извърши плащане в търговски обект или пък да получи пари в брой (на английски: *cash advance*).

• дебитна:

При дебитната карта средствата се изтеглят директно от банковата сметка на картодържателя или, ако тя позволява предварително зареждане със средства, директно от картата до изчерпване на средствата. Използването на дебитни карти е широко разпространено и измества в исторически план ползването на чекове. С тях може да се изтеглят пари в брой от банкомат, а някои търговци предлагат и услугата пари в брой при плащане на техните каси (на английски: *cashback/cashout*).

Обикновено банките предоставят на търговците информационни знаци с изобразени лога на обслужваните карти. Повечето ПОС терминални устройства познават картата още при прочитането и в случай, че не се обслужва, незабавно извеждат съобщение на екрана. Най-популярните видове карти са VISA, VISA Electron, MAESTRO, MASTERCARD. Обслужват се масово от повечето ПОС терминални устройства. По-малко популярни в България са American Express (или AMEX) и Diners Club. Съществуват и местни марки обслужвани само в страната (така наречените "DOMESTIC BRANDS")- EUROLINE, TRANSCART и други.

Защитни елементи на кредитни карти MasterCard и Visa

	MasterCard	**Visa**
1. Лого		 или 
2. Холограма	До логото на MasterCard в сребрист или златист цвят. Триизмерен образ, във вид на разгънат земен глобус на фона на редове с многократно изписани надписи MasterCard.	Триизмерен образ на гълъб. Ако картата е със старото лого, то холограмата е на лицевата страна до логото на Visa. При карти с новото лого на Visa, холограмата може да липсва от лицето и да е поместена на гърба й - върху цялата магнитна лента или на друго място на гърба на картата.
3. Символ MC (слепени) за MasterCard или релефна буква "V" за Visa	Разположен е винаги вдясно от релефно изобразената дата на валидност на картата и на една линия с нея. При карти, произведени след 1 юни 2006 г., е възможно този знак да липсва.	Първата буква от Visa, която е разположена винаги до релефно изобразената дата на валидност на картата и на една линия с нея. При карти, произведени след 1 септември 2005 г., този знак липсва.
4. Номер на картата	Релефен. Първата цифра винаги е "5", но е възможно картата да започва с "5" и да не е MasterCard, а Maestro дебитна карта.	Релефен. Първата цифра винаги е "4", но е възможно картата да започва с "4" и да не е Visa, а Visa Electron дебитна карта.
	Номерът се състои от 16 цифри, разделени в четири групи по 4. Първите четири цифри от релефния номер на картата се повтарят, в напечатан вид, точно под първата група цифри. последната група от 4 цифри е разположена върху холограмата.	

5. Име на картодържателя	Името и фамилията на картодържателя са нанесени релефно върху лицевата страна на картата под номера на картата.	
6. Дата на валидност на картата	Разположена над имената на картодържателя във формат месец, година (ММ/ГГили ММ/ГГГГ) или ден, месец, година (ДД/ММ/ГГ). Всяка карта е валидна до 24:00ч на последния ден от месеца, обозначен в датата на валидност.	
7. Име на банката-издател на картата	Изписано е в лявата горна част на лицевата страна на картата.	
8. Магнитна лента	Магнитната лента е разположена на гърба на картите	
9. VOID	1 Ако присъства надпис VOID върху полето за подпис, то картата е невалидна	
10. Поле за подпис на гърба на картата	Надпис MasterCard в редуващи се червен, жълт и син цвят под ъгъл 45°, върху който е принтиран под наклон номера на картата или само последните 4 цифри, както и трицифрен код CVC2, който се намира след цифрите от номера на картата. CVC2 кода може да бъде изписан в отделно бяло квадратче.	1 При старо лого - надпис Visa в редуващи се син и жълт цвят под ъгъл 45°, върху който е принтиран под наклон номера на картата или поне последните 4 цифри от него, както и трицифрен код CVV2, който се намира след тях. При ново лого - лентата за подпис е раирана с редуващи се райета в жълто и синьо; CVV2 кода може да бъде изписан в отделно бяло квадратче.

В заключение може да се посочи, че все по-често се използват банкови карти за различни транзакции. Употребата им е толкова масова, че няма как да се мине без проблеми при този вид разплащания. Освен това в момента са в процес на развитие и мобилните плащания, които предлагат повече удобства, но и нови предизвикателства, които ще бъдат предмет на последващо изследване. Наред с това устройствата за обработка на POS плащанията с кредитни и дебитни карти все повече стават удобни мишени за кибер престъпниците. Затова е необходим постоянен стремеж за повишаване сигурността на картовите плащания и изграждане на устойчиво потребителско доверие към ползването на карти от банките.

ЛИТЕРАТУРА:

1. Заводска, З., Иванич-Дроздовска, М.,Яворски, В., Банково дело.
2. http://www.ccbank.bg/
3. http://www.bobs.bg/
4. http://www.bobs.bg/bg/atms/%D1%82%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D0%B8
5. .http://haralanov.com/techno/payments/27-pos-terminalni-ustroistva
6. .http://computerworld.bg/34067_za_elektronnite_plashtaniya_i_horata
7. .http://payment.bank.bg/

ПРОЦЕС НА УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ ПРИ КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ КАТО ЕЛЕМЕНТ ОТ НАЦИОНАЛНАТА СИСТЕМА ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА

Стоян Г. Тонев

PROCESS OF MANAGEMENT OF THE INFORMATION SECURITY ABOUT CLASSIFIED INFORMATION AS AN ELEMENT OF THE NATIONAL SYSTEM FOR PROTECTING THE INFORMATION

Stoyan G. Tonev

ABSTRACT: The management of the classified information is a contemporary approach which application in the sphere of security allows protecting the national security

***KEY WORDS*:** Information security, classified information, types of protection of the classified information, the need to be known

Стратегическият приоритет на правителствата на Република България, с подготовката, влизането ни в Северноатлантическия алианс и Европейския съюзи в последствие, бе изграждането на унифициращa законодателна и институционална база в страната в областта на защитата на класифицираната информация. Целта е да се дефинират по нов начин приоритетите и основните понятия, да се определят компетентни органи и да се регламентират техните правомощия, детайлно да се уредят процедурите и принципите за защита на класифицираната информация, като се приведат в съответствие с политиките и стандартите на НАТО и ЕС, както и за изпълнението на споразуменията по сигурността между Република България с ЕС, НАТО и с други страни – членки и партньори. Политиката за сигурност на класифицираната информация може и трябва да бъде част от обща политика за информационна сигурност – както е в ЕС и НАТО, така да е и в Р. България.

В тази област приетият през 2002 г. закон за защита на класифицираната информация (ЗЗКИ) [1] създаде нова регулаторна рамка, съобразена с принципите за изграждане на модерната демократична държава. Законът въведе принципно нови понятия като „класифицирана информация", „физическа сигурност", „индустриална сигурност", „документална сигурност" и др. видове сигурност, дефинирани като основни за закона разпоредби, напълно съответстващи на стандартите на НАТО и на Европейския съюз.

„Документалната сигурност"е система от мерки, способи и средства за защита на класифицираната информация при създаването, обработването и съхранението на документи, както и при организиране на работата на регистратурите за класифицирана информация, което е основен управленски процес.

Със закона се въвежда принципът „***необходимост да се знае"*** **и** ***„видовете защита на класифицираната информация"*** за надеждност при създаване, съхранение, предоставяне на класифицирана информация и работа с такава, но слабо и непълно са засегнати критериите за управление на АИС и Мрежи, което се дължи както на технологичните новости, така и на липсата на единни критерии за ефекти-

вен управленски процес на защита на информацията.

Условията за защита на класифицирана информация, процедурите по видовете защита на класифицирана информация се уреждат в глава VI на ЗЗКИ, където са посочени ясни критерии за преценка на надеждността на шест вида сигурност на информацията, от гледна точка на сигурността и от гледна точка на опазване на тайната.

Управлението на видовете защита на класифицираната информация и оценката на възможностите за защита на класифицирана информация е сложен управленски процес, свързан със създаването, обработката и съхранението на разнородна и голяма по обем информация. Процесът, като неделим елемент от системата на защита на класифицираната информация, е един от основните фактори за нейната сигурност. В организационните единици /ОЕ/ се прилага утвърден модел на процес за защита на класифицирана информация, който е изостанал от технологичните новости и е предпоставка за ***„нерегламентиран достъп да класифицирана информация”***. Действащата процедура за определяне на сигурността често се определя като трудоемка и тромава. В този аспект, прилагането на информационните технологии води до рязко увеличаване на обмена на информация, която се обработва и използва за определено време. Това налага необходимостта от оценка и анализ на съществуващата практика и предлагане на нов, ефективен модел за оптимизиране на ***техническите и организационни*** изисквания по защита и управление на ***класифицираната информация***.

Оценката на тезите определят темата, като изключително ***актуална и значима***. Нейното разработване осигурява компенсирането на съществуващите процеси, в теоретично и практическо отношение, в организацията по управлението на класифицираната информация, което ще осигури:

1. разработване на надеждни процедури по създаване на класифицирана информация и нейната защитеност в АИС и Мрежи;
2. създаване на оптимизиран модел за управление на класифицираната информация за надеждност, спрямо сега действащия модел;

Разработването и внедряването в на система за ефективно управление на класифицираната информация и повишаване на непрекъсваемостта за надеждност, ще намали субективизма и ще осигури натрупване в информационен масив на данни, които могат да се анализират впоследствие и да послужат за определяне на рискове и заплахи за адекватна контраразузнавателна дейност по наблюдение, разкриване, противодействие, предотвратяване и пресичане на замислени, подготвени или осъществявани посегателства срещу националната сигурност (ЗДАНС) – чл. 4, ал. 2. [2]

Целта е на основата на обзорния анализ и на съществуващия опит и на специализирани публикации, да се обоснове теоретично, проектира и предложи за внедряване модел на процеса по управление и защита на класифицираната информация в АИС и Мрежи, както и използване на различни техники и технологии, с които да се осигури повишаване на оперативността на обработката, съхранението и обмена на необходимата класифицирана информация. Предоставяне на структурирано знание, методология и добри практики в областта на сигурността и защитата на класифицираната информация.

За постигането на тази цел, чрез публикацията се засягат решаването на следните **задачи:**

- оптимизиране на процеса по обработка на класифицирана информация по изведени показателни информативни критерии;

- изследване на подсистемата за надеждно управление на класифицираната информация, в контекста на общата теория на системата за сигурност на информацията, и определяне на нейния обхват;

- анализ на възможностите на информационните техники и технологии за усъвършенстване и оптимизиране на процеса по защита на класифицираната информация на отделните организационни единици (ОЕ);

- разработване на система за обработка на класифицирана информация и прилагането й в работата на организационните единици;

Обект на изследването е „националната **с**истемата за защита и управление на класифицираната информация", на база законодателството на страната в условията на реално членство на Р. България в ЕС и НАТО.

Предмет на изследване: Оптимизиране процеса по управление на класифицираната информация, като елемент от националната система за защитата на информацията.

Хипотеза на изследването: След анализа на процеса по създаване на класифицираната информация, да се унифицира процесът по създаване на единни правила и процедури в организационните единици. Да се разработи и внедри модел за надеждност при управление на класифицираната информация, което ще доведе до стандартизиране на процесите в модела, а оттам – до оптимизиране и автоматизиране на процеса по надеждна защита.

Управлението на класифицираната информация може и следва да се разглежда, използвайки системния подход. Изхождайки от общото определение, че системата е множество от елементи, които се намират в отношения и връзки помежду си и образуват определена цялост, може да се направи изводът, че системата за надеждно управление на класифицираната информация трябва да притежава следните характеристики:

- наличие на връзки и отношения между образуващите я елементи;

- неразривно единство със средата, във взаимодействие с която системата изразява своята цялост;

- разглежда се като система от по-висок порядък, докато нейните елементи могат да бъдат системи от по-нисък порядък;

- поведението й е подчинено на постигане на определена цел;

- цялостното й функциониране е резултат от взаимодействието между всичките й елементи.

В съответствие с гореизложеното, и прилагането на системния подход, който цели максимално обхващане и разглеждане на вътрешните и външни връзки за системата за надеждно управление на класифицираната информация, като подсистема на националната система за защита на класифицираната информация и националната сигурност.

На базата изложеното дотук, в теорията на системите и системния анализ се определят някои основни принципи [3].

Като първи принцип се обособява цялостност на системата с нейните две страни: 1) свойствата на системата (цялото) не са сума от свойствата на елементите й; 2) свойствата на системата (цялото) зависят от свойствата на елементите й, като изменението в една част води до изменение в цялата система. Свойството цялост-

ност е свързано с целта, за изпълнението на която е предназначена системата.

Вторият принцип е комуникативност. Този принцип стои в основата на определението за система и е подчинено на факта, че системата образува единство със средата. Всяка изследвана система е елемент от система от по-висок ранг, а елемент от изследваната система се явява система от по-нисък ранг, т.е системата не е изолирана, тя е свързана чрез множество комуникации както със средата, така и със собствените си елементи, което пък създава изисквания и ограничения за изследваната система. Основно съдържание на системния анализ е определянето на структурните, функционалните, информационните и пространствено-времевите връзки.

Третият основен принцип е свързан със свойството на системата ефективност. Теоретично е доказано, че винаги съществува функция ценност на системата, която зависи от нейната структура и функциониране. Процесът на изменение на състоянието на елемента (системата) се оценява по степента на постигане на целите, свързани с нейното функциониране.

Като четвърти принцип се определя управляемост на системата. Всяка система съдържа елементи (системи) за управление, които контролират съответствието между резултата на действие на системата и поставената цел. Елементите изпълняват, или са длъжни да изпълняват, целта точно колкото е зададена отвън – нито повече, нито по-малко (не малко или много, а оптимално), по принципа: „необходимо и достатъчно". Елементите на управление следят за изпълнението на целта.

Следователно системата управление на класифицираната информация се характеризира с:

– цел (определя предназначението на системата);

– йерархия (определя взаимоотношенията между всички елементи на системата без изключение);

– изпълнителни елементи;

– блок на управлението (следи за правилното протичане на действията за достигане на целта).

Не на последно място е принципът ***изоморфизъм.*** Той се състои в наличие на еднозначно или частично съответствие на структурата на една система на структурата на друга, което дава възможност да се *моделира* една или друга система с помощта на подобна на нея система.

Методът на системния инженеринг в най-пълна степен удовлетворява изискванията за комплексност и дълбочина при изследване проблематиката на сигурността. Прилагането на системния анализ дава възможност да се осветяват и разглеждат различни свойства на тези системи, техни особености и канали на проявление в различни условия на средата за информационна сигурност. Така не само анализаторите, а и лицата, вземащи решения, придобиват представа за мащабите на „цялото" и особеностите на „частното". Системният синтез дава възможност да се изследва взаимодействието между елементите в различните организационни единици, да се прогнозира тяхното поведение и да се предвиждат възможните резултати (ефекти) от използването на различни инструменти на политиката за сигурност на класифицираната информация в различни ситуации и за постигането на различни цели.

Обобщавайки, елементите на системата за защита на класифицираната информацията те се включват в националната система за защита на класифицираната информацията, която е комплекс от компетентни органи и мерки за осъществяване на специфични информационни, аналитични и контролни дейности, даващи въз-

можност за обединяване на информацията от организационните единици на територията на страната и чужбина[4].

Разглеждайки системата за защита на класифицираната информация е необходимо и изясняване на някои понятия и определения.

Класифицирана информация – видове

Сред множеството информация, която е защитена, централно място заема класифицираната информация (КИ). Това се дължи на факта, че интересите към нея са безспорни и опазването ѝ спомага за осигуряване на националната сигурност.

„Класифицирана информация", по смисъла на ЗЗКИ, е информация в три разновидности, представящи се като държавна тайна, служебна тайна, както и чуждестранна класифицирана информация[5].

Обектът на защита на *Държавна тайна* е информацията, определена в списъка [6] към ЗЗКИ, нерегламентираният достъп до която би създал опасност или би увредил интересите ни, свързани с националната сигурност.

В Списъка на категориите информация, подлежаща на класификация като държавна тайна, те са разделени според държавните интереси: информация, свързана с отбраната на страната, с външната политика и вътрешната сигурност на страната и информация, свързана с икономическата сигурност на страната. Смисълът от това информацията – държавна тайна да се отдели в категории е тя да бъде адекватно защитена. Само ***класифицираната*** информация получава необходимата защита със съответните мерки за защита като държавна тайна. В рамките на държавната тайна може да се установят нива за класификация за сигурност на информацията и съответен гриф за сигурност, който се определя от степента на увреждане и размера на вредите за националната сигурност, които ще нанесе нерегламентираният достъп до тази информация.

Обектът на защита на ***служебната тайна*** е информация, създавана или съхранявана от държавни органи или органите за местно самоуправление, която не е държавна тайна и която може да се отрази неблагоприятно върху интересите на държавата или да увреди друг правозащитен интерес. За да има списък от категория информация – служебна тайна, е необходимо да има специален закон, който база за ръководителят на съответната организационна единица да обяви списък с категориите информации, определени, като служебна тайна, за да регламентира дейността по защитата на служебната тайна на съответната организационна единица.

Съхранението на ***чуждестранната информация*** като класифицирана, чувствителна и др. информация се извършва по силата на сключени международни договори, които определят задължения по защитата на информацията или цели осигуряване на допълнителна защита, когато това се налага от характера на информацията ДКСИ по предложение на службите за обществен ред и сигурност може да определи с решение, допълнителни маркировки, специален ред за управление и кръга на лица с право на достъпдо нея.

На базата на тези определения (признаци) на видовете класифицирана информация, като обединяващо звено може да се определи засягането на определен държавен интерес, в резултат на нерегламентиран достъп. Понятието „нерегламентиран достъп до класифицирана информация" [7] е определено в закон и засяга разгласяване, злоупотреба, промяна, увреждане, предоставяне, унищожаване на класифицирана информация, както и всякакви други действия, водещи до нарушаване на защитата ѝ или до загубване на такава информация. За нерегламентиран достъп се

счита и всеки пропуск да се класифицира информация с поставяне на съответен гриф за сигурност или неправилното му поставяне, както и всяко действие или бездействие, довело до узнаване от лице, което няма съответното разрешение или потвърждение за това каквито са международните изисквания.

Система за защита на класифицираната информация е изградена на базата на посочените принципи и легално дефинира понятието **„Национална *система* за защита на класифицирана информация"** [8], като генералната цел на тази система е ***защита от нерегламентиран достъп***. Елементите на тази система са компетентните органи и прилаганите от тях мерки, насочени към защитата на класифицираната информация от нерегламентиран достъп. Разглеждането на тази система обхваща няколко аспекта: 1) наличие на законодателни и административни нормативни актове; 2) дейността на всички органи, имащи правомощия в областта на защита на класифицираната информация, като се търси необходимата координация между тях; 3) прилагането на установените мерки в отделните видове сигурност на класифицирана информация, които в тяхната цялост водят до постигане на защитата на класифицирана информация. Обединяващо звено между елементите на системата за защита на класифицирана информация е ***единодействието***, насочено към определена цел – защитата на класифицираната информация от нерегламентиран достъп [9].

Като се има предвид широкия спектър на възможните заплахи за сигурността на класифицираната информация в АИС и Мрежи, нейната защита трябва да бъде организирана системно и последователно. ЗЗКИ и подзаконовите актове по неговото прилагане, предвиждат система от органи, ангажирани със защитата на класифицирана информация и изграждане на система от мерки, чрез които тази защита ще бъде постигната. Адекватният отговор на заплахите за информационната сигурност е противодействието на тези заплахи, чрез установяване на една стабилна *система* за нейната защита, която функционира чрез изпълнение на правомощията на органите по защита на класифицираната информация и прилагане на система от нормативно установени правила за защита на класифицираната информация.

Анализът в тази посока сочи към разглеждане на защитата на класифицираната информация, като резултат от целенасочената дейност на оправомощените органи по прилагане на принципите, способите и мерките, включени в обхвата на различните видове информационна сигурност [10].

Елементите на системата за защита на класифицирана информация включват органите за защита на класифицираната информация, като в различни аспекти са ангажирани множество органи – Народното събрание, Президентът на Р. България, Министерският съвет, Държавната комисия по сигурността на информацията (ДКСИ), службите за сигурност, службите за обществен ред, организационните единици, служителите по сигурността на информацията и административните звена за сигурност, които могат да се изграждат към тях. Взаимодействието между органите, изпълнението на техните правомощия са фактори, от които зависи защитата както на класифицираната, така и на други видове защитена информация.

По силата на ЗЗКИ, ДКСИ е държавният орган, осъществяващ политиката на Р. България за защита на класифицирана информация. Комисията организира, осъществява, координира и контролира дейностите по защита на КИ и осигурява еднаквата й защита в национален мащаб. ДКСИ осъществява своята дейност в тясно взаимодействие с органите на ДАНС, Министерство на отбраната, Минис-

терство на вътрешните работи, Министерство на външните работи, службите за сигурност и за обществен ред.

За да бъдат разгледани по-обстойно, функциите на службите за сигурност се разделят на общи функции, т.е. такива, които касаят всички служби за сигурност и специфични функции.

Общите функции на службите за сигурност се свеждат до:

– Извършване на проучванията за надеждност на своите служители и на кандидатите за работа;

– Издаване на разрешения на служители и кандидатите за работа;

– Прекратяване на разрешения на своите служители;

– Отказване издаване на разрешение на кандидатите за работа;

– Отнемане на разрешения на своите служители и на кандидатите за работа;

– Извършване на проучвания на физически и юридически лица, които кандидатстват за сключване на договор, свързан с достъп до класифицирана информация;

– Извършване на проучвания на физически и юридически лица, които изпълняват договор, свързан с достъп до класифицирана информация;

– Издаване на удостоверение за съответствие с изискванията за сигурност, съгласно ЗЗКИ и проверки за задължителните мерки за сигурност на стратегически зони и режим на достъп до тях свързани с изпълнение на стратегически дейности.

Специфичните функции на службите за сигурност, в частност Държавна агенция национална сигурност (ДАНС), съгласно Закона за ДАНС, извършва дейности по защита на националната сигурност от посегателства срещу националната сигурност, свързани както с нарушаване функционирането на Националната система за защита на класифицираната информация, така и деструктивни въздействия върху комуникационни и информационни системи.

Мерките за защита на видовете информация се свеждат до държавната политика по защитата на информацията, касаещи системата от правила и мерки, регламентирани в нормативни актове, регулиращи защитата на чувствителна информация, нарушаването на които води до носене на отговорност.

Основополагащи актове в националното законодателство, свързани с информационната сигурност на АИС Мрежи **за класифицирана информация са:**

Закон за защита на класифицираната информация, от 2002 г.

Наредба за задължителните общи условия за сигурност на АИС или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация, приета с ПМС № 99 от 10.05.2003 г., обн. ДВ бр.46 от 20 май 2003г. и последно изм. ДВ бр.101 от 18 декември 2009 г.

Наредба за криптографската сигурност на класифицираната информация, приета с ПМС № 263 от 11.11.2003 г., обн. ДВ бр.102 от 21 ноември 2003 г. и последно изм. ДВ бр.5 от 19 Януари 2010 г.

Тази политика е във функциите и задълженията на Държавната комисия по сигурността на информацията. Контролни функции по спазването изискванията на посочените нормативни актове осъществява Държавната агенция „Национална сигурност".

Защитата на сигурността на класифицираната информация следва да се изгражда системно, да се обединяват различни принципи, способи и средства за противодействие срещу съществуващите заплахи. Това разнообразие води до изграждане на система от мерки по отделни видове сигурност на класифицираната информация.

Видове сигурност на класифицираната информация са определени от законодателя едностранно в ЗЗКИ и се отнасят до:

персоналната сигурност на класифицираната информация, която е свързана с *превантивно* изискване за установяване на надеждността на лицето и спазване на принципа „необходимост да се знае";

документалната сигурност на класифицираната информация, която е свързана със защитата ѝ при създаването, обработването, съхраняването, пренасянето на документи, както и организирането на работата на регистратури;

физическата сигурност на класифицираната информация, която е свързана с изграждането на физическа среда, където да се създава, съхранява и обработва класифицирана информация. В този смисъл физическата сигурност се изгражда на базата на система от организационни, физически и технически мерки, включваща защитата на сгради, помещения и съоръжения, контрол на достъпа върху тях, с цел да се предотврати нерегламентиран достъп до КИ;

индустриалната сигурност на класифицираната информация, която е свързана с изпълнението на договор, свързан с достъп до класифицираната информация – държавна тайна и цели установяване на надеждността на кандидатите за сключване на договор, изисквания към съдържанието на договорите, тяхното изпълнение и прекратяване;

Информационната сигурност, която е свързана с автоматизираните информационни системи или мрежи и криптографската сигурност на класифицираната информация е необходима по повод електронното създаване, съхраняване, обработване и обмен на класифицирана информация.

Гореизложеното налага извода, че защитата на КИ е постигната тогава, когато са приложени принципите, способите и мерките, попадащи в обхвата на видовете сигурност на класифицираната информация.

По смисъла на ЗЗКИ класифицираната информацията е защитена, когато са неутрализирани обозримите заплахи, пораждани от физическите носители на информацията, от лицата, които работят с нея, от помещенията, в които тя се съхранява и т. н.

Постигането на всяка от шестте вида сигурност е предпоставка за подобряване на защитата на класифицираната информация като цялостен процес, както за страната така и на партньорите ни, защото ЗЗКИ не прави разлика, както между видовете собственост така и за националността на защитаваната информация.

На база изводите се налага необходимостта от крищяща нужда от актуализация на законодателната и нормативната база за работа и управление на класифицирана информация чрез АИС и мрежи с цел да отговори на предизвикателствата на технологичното развитие на компютърните и комуникационни технологии към момента.

ЛИТЕРАТУРА:

1. Закон за защита на класифицираната информация (ЗЗКИ), Обн, ДВ бр.45/30.04.2002 г.

2. Виж.чл.4, ал.1, т.10 от Закона за Държавна Агенция Национална Сигурност (ЗДАНС)

3. Рубцов С. В., Взаимодействие открытах систем – старая концепция для новых идей. Новые рынки, 2001 l, N 4, 17-19

4. Правилник за прилагане на закона за защита на класифицираната информация, ДВ бр. 115, изм. ДВ бр.22/2003 г.
5. (ЗЗКИ), Обн, ДВ бр.45/30.04.2002 г.
6. по риложение 1 към Закона за защита на класифицираната информация
7. § 1, т. 6 от Допълнителните разпоредби на ЗЗКИ
8. Закон за ДАНС
9. Семерджиев, Ц., Проектиране на организациите, Военен журнал 2, 2005 г
10. Семерджиев, Ц., Проектиране на организациите, Военен журнал 2, 2005 г.

ОБЩИ ПОЛОЖЕНИЯ - ПРАВНИ СТАНДАРТИ НА КОМПЮТЪРНИ ПРЕСТЪПЛЕНИЯ

Стоян Г. Тонев

GENERAL CONDIOTION LAW STANDARTS CYBERCRIME

Stoyan G. Tonev

ABSTRACT: Working legislation of cyber crime is the best prevention

***KEY WORDS*:**Law standarts, cyber crime and electronic data

Ако 80-те години се залагаше на качеството, а 90-те – на инженеринга, то акцентът на 21-то столетие ще е върху скоростта на достъп и обработка на информацията в киберпространството. Промените в развитието на обществото настъпват вследствие на една обезоръжаваща проста идея: потока на дигитална информация. И тук, вече в 21 век, средствата и комуникативността на информационната епоха ни предоставят възможност за лесен достъп, разпределение и обработка на информацията по нови и забележителни начини.

Имайки предвид главоломното развитие на информационните и комуникационните технологии, не е чуждо подобряването на средствата за извличане на информация, за съхраняването й върху съвременни носители, повишаването на скоростта за предаване на информация, както и надеждността и сигурността на информационните системи. В никакъв случай не трябва да изключваме възможността от подводни камъни в Информационния океан.

Информационните и компютърните системи, мрежите и комуникационните устройства все по-бързо се развиват и стават все по – взаимосвързани. Тъй като обществото става все по-доверчиво и зависимо от информационния поток в тези мрежи неизбежна е нужда от автоматизирането на много дейности, което води след себе си увеличаване на възможността за нарушаване, манипулиране, разрушаване, унищожаване и кражба на данни /чувствителна информация/, намиращи се и разпространяващи се в тези киберсистеми. Това явление дава и голям брой термини: кибер-престъпление; компютърно престъпление, свързано с компютри и информационни технологии; и престъпление в сферата на високите технологии и информационната сигурност.

Глобалната уязвимост на световната мрежа се потвърждава посредством увеличаващия се брой актове на кражби, измами, повреди, промяна на чувствителни данни и програми, водещи след себе си парализиране на дейността и причиняващи загуби до особено големи размери, водещи след себе си висока обществена опасност за финансовата и икономическа сигурност, стабилност и устойчивост на институции и държави. Компютрите и Интернет добавят нов инструмент към арсенала с, който извършителите престъпление могат да боравят. Интернет предоставя възможност за достъп до всяка точка по света, анонимно и незабавно посредством сигурна комуникация, достъп до разнообразна чувствителна информация, с увеличаващи се цели и възможности за престъпления. Компютърните престъпления са добре познати престъпления, извършени с новите средства на компютърните и информационните технологии. Следва да се смята, че само по себе си компютърното престъпление не е престъпление в изолация, а формирано, като част от престъпление, което по един или друг начин е свързано с използването на компютърни и информационни технологии.

С развитието и разширяването на обхвата на компютърните системи и Интернет и приемането им в ежедневието на обществото, се увеличава и броят на неправомерните нерегламентирани достъпи и дейности. Обектите на евентуални атаки по целия свят са от национални и международни инфраструктури, военни, правителствени и образователни организации, големи корпорации, малки и средни предприятия, до компаниите предлагащи интернет продукти и услуги и техните потребители. Едно от най-големите предизвикателства, с които се сблъскват правораздавателните органи в борбата с международните компютърни престъпления, е тяхната **ефективна координация** в разследването, **предвид различните правораздавателни и съдебни системи в Европейския съюз, НАТО и ООН**. Като резултат от увеличения брой връзки в заобикалящата ни среда за сигурност, нараства все повече необходимостта и от по-точни критерии за **персонификацията** на лицата (субектите), с които установяваме контакт или с които се обменя чувствителна информация.

Електронните данни са източник на доказателство, които са обект или средство на престъпление. Това допринася за нови предизвикателства пред правораздавателните органи при залавянето, извличането и разглеждането на такива чувствителни данни. Задълбочени знания в разнообразието на технологиите и непрекъснато увеличаващия се размер на информационните носители на данни, извличането, изследването и анализа на данните водят до ефективен изход при разследването.

Бъдещето е дигитално, чиято същност е скоростта, като правораздаването е нужно да е в състояние да контролира ситуацията, предотвратявайки нещата да се случат, за да отговори на предизвикателствата на новото време.

Сигурността и защитеноста на информацията и поддържащите процеси, системи и мрежи са важни активи на всички организационни единици. Определянето, оценката, постигането, поддържането и подобряването на сигурността на информацията са съществени за повишаването на конкурентно способността, финансите, доходността за спазване на законите и поддържане на добрия имидж за организационната единица. Техните информационни системи и мрежи са изложени на заплахи за сигурността от голям брой контрагенти, включващи компютърна измама, шпионаж, саботаж, вандализъм, пожар, наводнение или други бедствия, аварии и катастрофи. Източниците на щети са все по-общи, по-амбициозни и сложни. В тази среда сигурността на информацията става все по-важна както за обществения, така

и за частния сектор на икономиката и за защитата на критичните инфраструктурни обекти и личността. В тези сектори гарантирането на сигурността на чувствителната информация дава възможност да се избегнат или намалят рисковете. Свързването на обществените и частни мрежи и споделянето на информационните ресурси увеличава трудността за постигане на ефективен контрол и безопасност върху тях. Тенденцията на развитие на разпределени компютърни мрежи води до намаляване на ефективността на централния контрол, осъществяван от специалистите. Гръбнакът на информационното общество – интернет, е емблематична рожба на конвергенцията [1]. Това гарантира още по-динамично развитие на информационните и комуникационните технологии през следващите няколко години, което ясно се откроява от „Digital Agenda", водеща инициатива в рамките на стратегията „Европа 2020" [2]. Съвременните технологии направиха възможно свързването чрез Интернет на компютри от всяка точка на земното кълбо в обща мрежа, бъдещи и анонимни мрежи, носещи със себе си проблеми, свързани с адресното пространство[3]. В резултат на обвързването на човешките дейности с тези технологии, се получиха много допълнителни предимства, но едновременно с това се появиха много непознати и неизследвани до този момент рискове[4] и заплахи[4].

В свързаното общество хората, познанието, връзките и информацията са в непрекъснат обмен, което позволява по-бързо развитие и изисква все по-подготвени кадри в сферата на сигурността на тези системи и управлението и защитата на обменяната чувствителна информация. Точно тази динамика провокира креативността и тя тласка и изисква иновации, неспирна трансформация и по-висока ефективност

Много информационни системи не са проектирани да осигурят сигурност на чувствителната информация. Сигурността, която може да се постигне чрез технически средства, е **ограничена** и трябва да бъде поддържана чрез съответни **управленски решения** и установени процедури.

Определянето кои видове контрол трябва да се използват изисква детайлно планиране и отчитайки характеристиките на подробностите на системата за сигурност и конкретно информационната сигурност.

Управлението на сигурността на чувствителната информацията изисква, минимум участие на всички служители в организационните единици. То може също така да изисква участие на акционерите, доставчиците, трети страни, контрагенти. Може също така маже да изисква необходим съвет на експерт от външна организационна единица предвид спецификата на чувствителната информация ползвана в публичния сектор.

Общите правни стандарти за превенция на кибер престъпленията поставят своето начало с 50-то заседание на Европейският комитет по проблемите на престъпността през месец юни 2001г., като междуправителствен орган от експерти към Комитета на министрите на Съвета на Европа при които е приет окончателния проект на Конвенция за престъпления в кибернетичното пространство [5]. На 23.11.2001г. в Будапеща е официалното подписването на Конвенцията, на която присъства и министърът на правосъдието на Република България. На 19.09.2002г. Законопроектът за ратифициране на Конвенцията за престъпления в кибернетичното пространство е разгледан от Комисията по правни въпроси към 39-то Народно събрание. Конвенцията е ратифицирана със закон приет от 39 НС на 01.04.2005г. и обнародван в ДВ бр.29/25.04.2005г. и издадена от Министерство на правосъдието , публикувана в ДВ бр.76/15.09.2006г. и влязла в сила от 01.08.2005г.

Тази Конвенция е първият международен договор за престъпления, извършени по Интернет и други компютърни мрежи. Тя регламентира главно правонарушенията, свързани с авторските права, компютърната измама, детската порнография, както и с правонарушенията, свързани със сигурността на мрежите. Конвенцията съдържа правна уредба и на редица процедурни правомощия, като претърсване на компютърни мрежи и прихващане на информация. Основната цел на Конвенцията за престъпленията в кибернетичното пространство е постигането на „обща наказателна политика, насочена към закрила на обществото срещу кибернетичните престъпления, включително и чрез прилагане на съответното законодателство и поощряване на международното сътрудничество".

Търсенето на наказателна отговорност за предвидените в Конвенцията правонарушения е обусловено от две кумулативно дадени общи условия-инкриминираното поведение трябва да е извършено с умисъл и без законно основание.

Правонарушенията, които са предвидени в Конвенцията за кибернетичните престъпления, са обособени в четири категории:

- Правонарушения, свързани с тайната, неприкосновеността и осигуряването на достъп до данните и системите – незаконен достъп, незаконно прихващане, посегателство срещу неприкосновенността на данни, посегателство срещу неприкосновеността на системата, злоупотреба с устройства;
- Компютърни престъпления – компютърна фалшификация и измама;
- Правоотношения свързани със съдържанието: производството, разпространението и притежаването на детска порнография;
- Правоотношения свързани с авторските и сродните им права: масово разпространение в големи мащаби на незаконни копия от произведения, закриляни от авторското право.

В Конвенцията са посочени основните правила, които ще улеснят разследването във виртуалния свят и които представляват нови форми на правна помощ. Процесуалноправните разпоредби на Конвенцията въвеждат стандарти по отношение на разследването на определените в нея кибернетични престъпления и по-конкретно:

- запаметяване на съхраняваните данни;
- запазване и бързо разгласяване на данните, свързани с трафика;
- претърсване на системите и изземване на компютърни данни;
- събиране в реално време на данните относно трафика;
- прихващането на данни, свързани със съдържанието.

Въвеждането на процесуално – правните разпоредби от Конвенцията във вътрешното право трябва да е подчинено на условията, предвидени в законодателството на държавите – страни по Конвенцията, като се гарантира спазването на правата на човека и прилагане на принципа на **пропорционалността**. В този смисъл процедурите могат да се прилагат само при определени условия, като например необходимостта от предварително разрешение от съдебен или друг независим орган. В съответствие с вътрешното си право, с Конституцията на Република България, с Наказателно – процесуалния кодекс и със Закона за специалните разузнавателни средства, нашата страна е направила допустимата от чл.14, ал. 3 на Конвенцията резерва, че ще прилага разпоредбите, предвидени в чл.20 на Конвенцията, а именно прихващане на данните за трафика на компютърните съобщения, само по отношение на тежките престъпления, така, както те са определени в българския

Наказателен кодекс. Принципът за пропорционалност в българското законодателство е изразен непосредствено в разпоредбите на чл. 40, ал. 1 от Закона за електронните съобщения [6] по следния начин: „исканията на Комисията за регулиране на съобщенията за предоставяне на информация трябва да бъдат пропорционални на целите, за които са направени".

Възможно е да се изведе изводът, че използването и прилагането на специални разузнавателни средства /СРС/ представлява дейност, с която се реализира държавна принуда по отношение на конкретни правни субекти. Целта е предотвратяване, разкриване и доказване на тежки престъпления, което обуславя социалната ценност на принудата и нейната достъпност, във връзка със конституционните права и свободи на гражданите, във връзка с чл. 34, ал. 1 от Конституциятя ня Р.България. [7]. В тези случаи информацията не е класифицирана, но попада в категорията „чувствителна информация".

В Конвенцията се регламентират нови форми на международно сътрудничество в наказателно-правната област, съответстващи на правомощията, залегнали в нейните разпоредби. Така например, съдебните органи и службите по издирване на доказателства в електронна форма могат да действат по молба на държава-страна по Конвенцията, без да водят самостоятелно разследване или трансгранично претърсване. Получените данни трябва да бъдат предавани бързо.

Ратифицирането на Конвенцията се обуславя, от една страна от универсалния й характер, а от друга – от нейното значително голямо значение за предотвратяване на тероризма чрез Интернет. Важно значение има и фактът, че този международен договор предоставя адекватни средства за защита и предотвратяване на престъпленията, извършвани чрез компютърните системи и по компютърен път. Ратифицирането и обвързването с Конвенцията е и в съответствие с Резолюцията, приета на 24-та среща на министрите на правосъдието от европейските страни /проведена през м. октомври 2001г. в гр.Москва/ за укрепване на превенцията и наказанието на терористичните актове, извършени срещу или чрез компютърни и телекомуникационни системи /кибертероризъм/.

Правната уредба касаеща компютърните престъпления;

Международна нормативна уредба е свързана със:

-Конвенция за престъпления в кибернетичното пространство;

-Препоръка №R/89/9 относно престъпността свързана компютрите, която предлага на националните законодателни органи ръководните принципи при определянето на някои форми на компютърна престъпност;

-Препоръка №R/95/13 относно проблемите на наказателното производство, свързани с компютърните технологии;

-Европейска конвенция за законова защита на услуги, базирани на или представляващи условен достъп, ратифицирана със закон, приет от 39-то НС на 05.06.2003г. /ДВ бр.55/17.06.2003г./, влязла в сила от 01.07.2003г.

-Европейска конвенция за взаимопомощ по наказателно правни въпроси /в сила за Р България от 15.09.1994г./

-Европейска конвенция за екстрадиция /в сила за Р България от 01.10.1994г./

Българско законодателство регламентира компютърните престъпления чрез:

- Наказателен кодекс;
- Наказателно – процесуален кодекс;

- Закон за авторското право и сродните му права, обн. ДВ бр.56/93г. изм. и доп. в ДВ бр.77/2002г., в сила от 01.01.2003г.

- Наредба за секретните патенти, приета с ПМС 175/09.09.1993г.

- Закон за електронния документ и електронния подпис, обн. ДВ бр.34/2001г.

- Закон за далекосъобщенията, обн. ДВ бр.93/1998г.

- Закон за защита на класифицираната информация, обн. ДВ бр.45/30.04.2002г.

- Закон за защита на личните данни, обн. ДВ бр.1/2002г.

- Закон за специалните разузнавателни средства, обн. ДВ бр.95/97г. изм. и доп. в ДВ бр.17/02.12.2003г.

Международна правна помощ.

В чл.23 на Конвенцията за престъпления в кибернетичното пространство са регламентирани общите принципи на международното сътрудничество: „Страните си сътрудничат помежду си във възможно най-широка степен, в съответствие с международно правни актове за международно сътрудничество по наказателно правни въпроси, на установените договорености въз основа на еднакви или реципрочни законодателни разпоредби, и на вътрешното си право, за целите на разследването и на производството относно престъпления, свързани с компютърни системи и данни или с цел събиране на доказателства в електронен вид за дадено престъпление".

Взаимопомощта обхваща следните аспекти:

1. Взаимопомощ в областта на предварителните мерки: бързо запазване на съхраняваните компютърни данни, намиращи се на територията на помолената за помощ държава /чл.29 от Конвенцията/; бързо разкриване на запазени данни /чл.30 от Конвенцията /.

2. Взаимопомощ относно правомощията за разследване: взаимопомощ по отношение на достъпа за съхраняваните компютърни данни /чл.31 от Конвенцията /; транзграничен достъп до съхраняваните данни със съгласие или в случай, че те са общодостъпни /чл.32 от Конвенцията /; при събирането в реално време на данни за трафика, отнасящи се до конкретни съобщения, предадени с помощта на компютърна система /чл.33 от Конвенцията /; взаимопомощ в областта на прихващане на данни относно съдържанието /чл.34 от Конвенцията /.

В съответствие с Конституцията на РБългария, с НПК и със ЗСРС, че в съответствие с вътрешното ни право, нашата страна е направила допустимата от чл.14, ал.3 от Конвенцията резерва , че ще прилага разпоредбите предвидени в чл.20 от същата, а именно прихващането на данни за трафика на компютърните съобщения само по отношение на тежките престъпления, така както те са определени в Наказателния кодекс на РБългария.

С оглед бързото събиране на доказателства в електронна форма за дадено престъпление, Конвенцията допуска в неотложни случаи, молбата за взаимопомощ или съобщения свързани с нея, да бъдат отправяни до помолената за съдействие държава, чрез най-бързите средства за комуникация, включително факс или електронна поща, доколкото тези средства дават достатъчна степен на сигурност на информацията и на автентичност на съдържанието/вкл. и използване на криптиране, когато това е необходимо/, с последващо официално потвърждение, ако замолената държава изисква това.

Ако не съществува разпоредба в обратен смисъл, изрично предвидена в чл.25 от Конвенцията, взаимопомощта се подчинява на условията, подчинени на вътрешното право на помолената за съдействие страна или в приложимите договори

за взаимопощ, включително и по отношение на основанията, на които замолената страна може да откаже сътрудничество.

Съгласно чл.464 от НПК, поръчката за правна помощ се изпраща до Министерство на правосъдието, освен ако в международния договор по който РБългария е страна, е предвиден друг ред. В съответствие с тази разпоредба ВКП има разпоредени писмени указания за изготвяне на следствени поръчки за чужбина, с цел извършване на отделни следствени действия или предаване на предмети, сведения и документи. В поръчката за правна помощ се съдържат данни за: органа, който я прави; предмета и мотива на искането; имената и гражданството на лицето за което се отнася искането; при необходимост – обвинението и кратко изложение на фактите по него.

Гореизложеното налага извода, че държавната намеса за защита на чувствителната информация е необходима в едно демократично общество, в интерес на националната сигурност и обществения ред, на икономическото благоденствие на Р. България на правосъдието, морала и здравето, подчинено на цялостната концепция за постигане на конкурентно предимство за предотвратяване на деструктивни въздействия и разкриване и събиране на годни доказателствени средства за извършени или подготвяни престъпления.

Като насоки на работа е наложително изискването за все по-подготвени кадри в сферата на управлението и защитата на чувствителна информация на база непрекъснатия обмен на информация в свързаното общество, познанието и връзките им. Точно тази динамика провокира креативността и тя тласка и изисква иновации, неспирна трансформация и по-висока ефективност на защитеност на информацията.

ЛИТЕРАТУРА:_

1. Състояние на приближаване на сходства – становище на експминистър Антони Славински – преподавател в Нов Български университет и председател на Асоциация „Телекомуникации” в сп. Икономика-бр.20, декември 2012 г.
2. www.ekonomymagazine.bg, декември 2012 г
3. Развитие на анонимните мрежи и аспекти на сигурността в бъдещите мрежи. Славянов, К.,. Николов, Л.
4. (ISO (IEC 17799:2005)Практически кодек по управление на информацията. **Риск** – комбинация от вероятността за настъпване на нежелано събитие и неговите последици (възможни щети или нанесен ущърб, загуби. **Заплаха** – потенциална причина за нежелан инцидент, резултата от който е във вреда на организацията
5. Конвенция за престъпления в кибернетичното пространство Обн, ДВ 76/15.09.2006 г.
6. Закон за електронните съобщения Обн, ДВ бр.45/30.04.2002 г
7. Бояджиев Н., Сп. „Съвременно право”, кн.5, 1999 г., стр.48
8. Адресите за кореспонденция :

КОНТРАБАНДАТА И НЕЛЕГАЛНОТО РАЗПРОСТРАНЕНИЕ НА НАРКОТИЦИ В РЕПУБЛИКА БЪЛГАРИЯ

Велико П. Петров

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "В. ЛЕВСКИ", ФАКУЛТЕТ "АРТИЛЕРИЯ, ПВО И КИС", КАТЕДРА "ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ТАКТИЧЕСКИТЕ ПОДРАЗДЕЛЕНИЯ ОТ ПОЛЕВАТА АРТИЛЕРИЯ" ГР. ШУМЕН

SMUGGLING AND ILLEGAL DISTRIBUTION OF DRUGS IN BULGARIA

Veliko P. Petrov

ABSTRACT: *This report aims to acquaint the reader with the most common activity in the structures of organized transnational crime, namely smuggling and illegal distribution of drugs. Knowing the seriousness of this problem every country in the world has created its specialized structures whose main tasks are to combat the production and distribution of drugs.*

KEYWORDS: *smuggling, illegal distribution of drugs.*

Българското общество през последните години е принудено да търпи жестоките последствия от разрастващия се пазар на наркотици, както и свързаното с това нарастване на броя на наркопрестъпленията. Темата за разпространението и потреблението на наркотични вещества придоби трайно присъствие в българското медийно пространство. Наркопрестъпността влияе негативно на много сфери на обществения и социалния живот и е един от факторите, застрашаващи сигурността и здравето на обществото. Тя е един от престъпните феномени, оценявани като заплаха не само за Република България, но и за страните от Европейския съюз. Трафикът на наркотици и свързаното с него разпространение са едни от най-доходоносните престъпни дейности, които имат структуроопределящо значение за организираната престъпност като цяло.

България е най-вече транзитна страна по отношение на наркотичните вещества. Основен фактор, който предопределя ролята на българската организирана престъпност, е географското местоположение на страната: както на „Балканския път" на хероина (от Афганистан към Западна Европа), така и на синтетични наркотици и прекурсори (от Европа към Близкия изток). Български граждани участват в международни престъпни мрежи, които се занимават с трафик на кокаин от Южна Америка (включително и през Африка) към Европа. Въпреки че участието е най-вече на средно и ниско равнище, съществуват изключения, които създават реална заплаха страната ни да се използва като транзитна дестинация за трафик на кокаин към Западна Европа.[1]

1 Оценка на заплахите от тежка организирана престъпност, Център за изследване на демокрацията, 2010 г. - 2011 г., стр. 28.

Глобализацията значително повиши трансграничния характер на организираната престъпност, като съвременните средства за комуникации създават условия за изграждане на престъпни организации от мрежов тип. Геостратегическата специфика на нашия регион, пресичан от пътища, свързващи Европа и Азия, естествено се вписва в маршрутите, използвани от международната престъпност. Географското разположение и възможностите, които членството в ЕС предоставя на част от страните, пораждат допълнителен интерес от страна на трансгранични криминални мрежи за нелегален трафик на наркотици, хора, оръжие и стоки[2].

Терминът контрабанда има италиански произход и се състои от словосъчетанието "*контра*" означава срещу и "*бандум*" означава правителствено разпореждане. **Контрабандата** *е дейност по пренасяне на пари, стоки или ценности през държавната граница в нарушение на установения от компетентните органи ред. Тя е винаги противозаконна, засяга интересите на повече от една страна. и е насочена срещу икономическия ред.* Пренасянето включва физическото действие по преместване местонахождението на контрабандните стоки през една или повече национални граници, но включва превозването или прехвърлянето през границата на такива стоки, когато се използва превозно средство, пътници и други, без контрабандиста да е във физическо съприкосновение с пренасяната стока. С понятието контрабанда се означава незаконното пренасяне през граница на стоки, ценности и други забранени за изнасяне, внасяне или транзитиране на предмети. През последните години, този термин се заменя с термина ***трафик***. В основата на дейността контрабанда е транзитирането на стоките – незаконен трафик (на наркотични вещества, на хора, на откраднати предмети на културата, на откраднати превозни средства и други). С контрабандата се нарушава суверенитетът на една или повече държави, засяга се икономиката и икономическите отношения между държавите. Контрабандата се извършва с цел да се реализира печалба. Най голямо разпространение има контрабандата в икономически и социално нестабилните райони. Контрабандата се извършва от лица с голям международен опит и е многостранно явление. Тя засяга административноправни и наказателноправни забрани. Развива се в страни с либерален режим на експорт и импорт и слаба финансова система и засяга почти всички сфери на обществения живот.

Трафикът на наркотици е най-доходоносната нелегална дейност. Половината от приходите от трансгранична престъпна дейност идват от трафик на наркотици. По изчисления от този бизнес оборотът в света е от около 320 млрд. долара на година. Парите, които се печелят са еквивалент на 0.6 – 0.9 % на глобалния БВП. Най-доходни са кокаин и хероин.[3]

Потенциалните рискове и заплахи от незаконния трафик, производство и търговия с наркотични вещества, запазват актуалното си значение. Българските наркоструктури са добре интегрирани в транснационални криминални организации. Те се включват в трафика на хероин за Западна Европа като подизпълнители главно на турски и албански наркотрафикантски организации. В сътрудничество с наркотърговци от Близкия Изток изграждат самостоятелни канали за трафик на

[2] Заместник–министър на вътрешните работи Димитър Георгиев, "Трансгранична престъпност и международно сътрудничество", Национална конференция, 30 и 31 януари 2012 г., Централен военен клуб – гр. София, стр.2.

[3] Най доходоносните престъпни дейности http://profit.bg/news/Naj---dohodonosnite -prestupni -dejnosti/nid-111020.html

синтетични наркотици, основно амфетамини. В производството си партнират с престъпни синдикати от Югоизточна Европа. Наркопрестъпността в страната е тясно свързана с наркотрафика. Рисковете от разширяване на предлагането и употребата на наркотични вещества намират израз в тенденцията на криминализиране на определени социални групи - непълнолетни, млади пълнолетни, роми. Средства за дрога по правило се набавят чрез извършване на криминални престъпления срещу собствеността на гражданите, а зависимостта от наркотици се използва от наркоорганизациите за упражняване на контрол върху доходоносни сфери на конвенционалната престъпност и за „поръчково" извършване на престъпления.

Произведените в една страна наркотични вещества най-често се пласират в други страни. Това е така особено заради характерните климатични изисквания на някои от растенията, които виреят добре на ограничени географски ширини. Наркотичните вещества се превеждат през границата на страните без знанието на митницата чрез различни способи, но най-често се скриват в големите контейнери на корабите, които доставят хранителни и други стоки, скриват се в специално пригодени чайници в моторни превозни средства, пренасят се от пътници в ръчния им багаж или погълнати. Действително, ефективността на борбата срещу наркотиците би трябвало да е в правопропорционална зависимост от действията на държавата не толкова срещу притежанието, колкото срещу трафика и разпространението им.

Наркотрафикът е част от наркоиндустрията, в която освен него се включват наркопроизводството и наркотърговията на дребно. Редица международни и нормативни актове определят наркоиндустрията като *незаконен трафик.* Наркотрафика в по-тесен смисъл означава: транзитиране, пренасяне, превозване, придвижване, прекарване, прехвърляне, претоварване, преместване, транспортиране, товарене, разтоварване, складиране на наркотични вещества и прекурсори, технологии и оборудване на територията на страната или през границите на държавите. Престъпните мрежи (контролирани от бившите силови групировки) са монополизирали наркотрафика и случайните лица в тази престъпна дейност веднага се отстраняват от тях. При конфликти, свързани с елиминиране на конкуренцията, се използват силови действия, съпроводени с бруталност и агресивност, и извършване на тежки криминални престъпления, включително и с общоопасни средства. Престъпните структури използват защитни практики, които гарантират минимални възможности за задържане на техни дилъри с дрога с цел запазване целостта на организацията при евентуални арести. Местата за размяна на стоката и парите непрекъснато се променят, членовете на организацията от различни йерархични нива не се познават помежду си, представят се с други имена, ползват автомобили и телефони на други лица, като ги разменят помежду си и т.н. Тази затвореност на структурите на доставчици и пласьори затруднява негласния контрол върху тях. Част от световния наркотрафик е контрабандата по Балканския път, включително на и пред територията на България.

Наркотичните вещества са разнообразни по своето съдържание и въздействие при тяхната употреба. Повечето от тях оказват моментално изключително силно влияние у хората, като продължителното приемане на какъвто и да е наркотик води до силно пристрастяване и зависимост. Наркотиците предизвикват трайни, трудно лечими здравословни проблеми, често и смърт.

В началото на XX век употребата на наркотици в България е рядкост. Позната е употребата на канабис и на опиумен мак, но рядко надхвърля границите на меди-

цинската употреба. В Югозападна България и други региони традиционно се е отглеждал за износ опиумът (афинът). С началото на масовата урбанизация тази традиция е прекъсната. До 60-те години на миналия век, употребата на нелегална дрога у нас е изключение.

В края на 60-те години на XX век се появяват първите случаи на немедицинска употреба на опиати сред млади хора, като за начало се счита Световният младежки фестивал в София 1968 г. Българските участници във фестивала за първи път се сблъскват и опитват от „химията на удоволствието". Това е времето на световната алтернативна младежка култура, започнала от САЩ и Западна Европа и превзела целия свят. 70-те години бележат началото на строг контрол над наркотичните вещества от страна на държавата. Употребяващите търсят лекарства и вещества, които не са под контрол. До 1990 г. България макар и транзитна страна, до този момент е била изключително изолирана от модата и културата на приемането на наркотици и не са били налице предпоставки за тяхното разпространение. В този период легално се е произвеждал амфетамин, който се е употребявал от студенти при изпити, като подобряващ концентрацията и умствената работоспособност.

През 90-те години на XX век е началото на хероиновия период в България. Употребяващи хероин са група иранци, живеещи в София и „ентусиасти" използващи наркотици (около 2000 човека) са първите опитали от най-смъртоносния наркотик. Употребата на хероин се превръща в епидемия. Доставките по това време са ставали предимно през Турция, не са били особено организирани, хероинът е бил сравнително чист и евтин. Използвани са множество арабски фирми за търговия на едро и дребно, които са внасяли освен декларираните продукти и хероин.

В периода от 1995 г. до 1997 г. силовите групировки СИК и ВИС-2 демонстративно се противопоставят на разпространението на хероин и има свидетелства, че тогава възникват първите контакти с организираните престъпни световни мрежи. Отстраняването на много от силовите застрахователи след нормирането на застраховането през 1997 г. кара същите да пренасочат дейността си към трафика на наркотици. През 2000 година голямо влияние оказва поставянето на Косово под специално международно управление и свръхпроизводството в Афганистан. Заплащането за осигурения канал е ставало чрез част от пратката, която е трябвало да се пласира на вътрешния пазар. След 2003 г. са убити двама ключови, организатори (босове) на трафика и разпространението на наркотици в България – Константин Димитров (Самоковеца) и Методи Методиев (Мето Илиенски), което дава възможност на тяхно място да се издигне Златомир Иванов (Златко баретата) и да създаде стройна организация известна като „Фирмата". Новото при „Фирмата" е силната йерархична структура, характерни за един организиран престъпен конгломерат. През 2009 г. след държавния натиск и последвалите арести и обвинения на над 20 членове на групировката, път си проправят нови фигури.

Леките дроги бележат плавно нарастване на употребяващите ги след 90-те години. Благоприятни се явяват подходящите климатични условия за отглеждане на канабис. Амфетаминът е дрога с история и традиции в легалното производството в България, като страната ни се явява износител предимно за арабските страни. В последствие България подписва международни споразумения, с които амфетаминът се поставя в списъка с наркотиците. Въпреки споразуменията след 1990 г. производството на амфетамин не е напълно преустановено, а складовете на фармацевтичните предприятия са били пълни. Според българските специални служби

останалият амфетамин се е изнасял чрез старите арабски контакти, като след приватизацията на дружествата, създадените от държавата „неофициални канали" за доставки се поемат от участниците в приватизацията. Българският амфетамин е с познато качество, приготвен от квалифицирани химици с опит в тази област и пласиран по разработените канали. България и Полша са най-големите производители и износители на амфетамин за Европа.

През последните години се наблюдава известна динамика в основните показатели за употребата на наркотици в България, което съответства на общите тенденции в Европейския съюз. По данни от Годишния доклад за 2007 г. по проблемите на наркотиците и наркоманиите, около 345 000-360 000 български граждани от 15 до 64 години поне веднъж в живота си са употребили някакво наркотично вещество. Най-масово използвания наркотик е марихуаната. Хероинът е най-силно свързания с проблемна употреба наркотик. Нараства употребата на синтетичните стимуланти - амфетамини и вещества от типа на екстази. При употребата на кокаин се наблюдава тенденция на леко увеличение.[4]

Тенденции в употребата на наркотични вещества:

1) Нарастване употребата на наркотични вещества сред младите хора и най-вече сред учениците - младите хора на възраст между 15 и 34 години представляват около 88-90% от всички лица във възрастовия диапазон 15-60 години, които поне веднъж в живота си са употребили някакъв наркотик. Всеки трети от студентите и учениците от 9-ти до 12-ти клас поне веднъж в живота си е пробвал наркотични вещества;

2) Снижаване възрастта на първа употреба – от употребяващите наркотици, приблизително 10 % са на възраст от 8-14 години;

3) Проблемна употреба на наркотици – броят на проблемно употребяващите хероин в България е между 20 000 и 30 000 лица с тенденция към намаляване, нараства употреба на марихуана, нараства броя на употребяващите синтетични стимуланти;

4) Здравни последици от употребата на наркотици – увеличава се броят на новорегистрираните и нараства броя на смъртните случаи свързани с употреба на наркотици.

Анализите на работещите в тази сфера български изследователи, полиция и специални служби показват, че наркоупотребяващите в страната ни са една хомогенна група и се подразделят по два критерия:

1) свързан е с типа наркотици, които се използват;

2) свързан е с начина на употреба и наличието на зависимост.

Според вида наркотиците в страната може да се различат три относително независими един от друг пазар на:

- меки дроги (*канабис, марихуана, хашиш и др.*);
- синтетични наркотици (*амфетамини*);
- хероин.

В съответствие със законовите им функции и задачи, правоприлагащите органи, митническите органи и специализираните служби на МВР осъществяват ефективни действия за ограничаване на наркотрафика и наркопрестъпността в страната, в резултат, на което през последните години същите постигнаха високи резултати в борбата срещу незаконното производство и трафик на наркотици и прекурсори.

[4] Национална стратегия за борба с наркотиците 2009-2013 г., стр. 4.

Борбата с разпространението на наркотици и тяхната употреба се извършва[5]:

1. Разработване на нормативна уредба за контрол върху наркотичните вещества и прекурсорите за санкциониране на свързаните с тях престъпления.

2. Периодична актуализация на списъка на наркотичните вещества и на суровините за тяхното производство.

3. Разработване на програми за ограничаване на производството, предлагането и търсенето на наркотични вещества. Разработване на ясни правила и ефективни механизми за контрол върху използваните химически субстанции в предприятията от химическата и фармацевтичната промишленост.

4. Разработване на комплексна програма за предотвратяване опитите за използване територията на страната като транзитен пункт за международен трафик на наркотици, упойващи вещества и суровини за тяхното производство, включваща и мерки за своевременното пресичане на наркоканали, организирани от български и чужди граждани.

5. Създаване на оптимална организация по своевременното установяване и унищожаване на нарконасаждения.

6. Разработване на стриктни правила за търговия на едро и дребно с лекарствени средства и субстанции с възможно наркотично въздействие.

7. Разработване и провеждане на програми за ограничаване на условията и факторите, способстващи за наркопотреблението, особено сред рисковите социални групи и територии; за ресоциализация на лица, пристрастени към употреба на наркотични и психотропни вещества.

8. Създаване на условия за обществена непримиримост към употребата на наркотици чрез активна информационна политика

За овладяване на проблема с наркотиците в България е необходимо да се обединят усилията на институциите на държавно, регионално и местно ниво, и да се съчетаят с усилията на неправителствените организации, медиите и широката общественост. Без съмнение, решаването на проблемите, свързани със злоупотребата и разпространението на наркотици, не може да бъде отговорност на една институция. За тяхното преодоляване са необходими съвместните усилия на цялото общество.

Изводи:

1) Наркотрафикът е най разпространената дейност в структурите на организираната транснационална престъпност и представлява дейност по внасяне или изнасяне в една или друга страна на наркотични вещества или суровини. Престъпната дейност в тази сфера се свежда до производството, търговията и употребата на наркотици. Наркоиндустрията е извън законите на всички съвременни държави. Пътят от производителя до отделния потребител е много дълъг. Търговията с наркотици се извършва на определени черни пазари. Международния трафик на наркотици се извършва по нелегални канали.

2) Наркотрафикът е процесът, от който зависи наркопроизводството и търговията с наркотични вещества. За изграждането на неговата стабилност и прогресивно развитие, са обособени престъпни организации по целия свят, които действат при висока конспиративност и създават силни позиции, както по отношение разпрост-

[5] Единна национална стратегия за противодействие на престъпността

ранение на наркотиците, така и сред институциите, които се борят за неговото противодействие.

3) Познавайки сериозността на проблема наркотрафик, всяка държава по света е създала свои специализирани структури, чиито основни задачи са свързани с борбата срещу производството и разпространението на наркотични вещества. Резултатите от тяхната дейност са налице, установяват се местата на производство, пътищата по които минават наркотиците, търговците и посредниците на наркотичните вещества. Освен специални служби, се използват и други методи за противодействие на наркотрафика.

4) Нормативните актове, инкриминиращи престъпния състав на тази дейност, водят до сериозни санкции за извършителите. Създадени са превантивни програми, които имат за цел да предизвикат сред хората, негативно мнение и ефект на всички нива (производство, разпространение, търговия и употреба на наркотични вещества). Държавите по света също се обединяват в борбата с наркотиците. Провеждат се съвместни мероприятия, семинари, операции, с цел успешното противодействие.

5) Въпреки множеството усилия, вложени в борбата срещу тази противоправна дейност, тя продължава да съществува. Необходимо е усилията на компетентните страни постоянно да се усъвършенстват и да придобиват колкото се може по-мащабен характер. По този начин ще се постигнат още по-добри резултати срещу един от най-големите врагове на съвременния свят.

ЛИТЕРАТУРА:

1. Оценка на заплахите от тежка организирана престъпност, Център за изследване на демокрацията, 2010 г. - 2011 г.

2. Димитър Георгиев, "Трансгранична престъпност и международно сътрудничество", Национална конференция, 30 и 31 януари 2012 г., Централен военен клуб – гр. София, стр.2.

3. Най доходоносните престъпни дейности http://profit.bg/news/Naj---dohodonosnite - prestupni-dejnosti/nid-111020.html

4. Национална стратегия за борба с наркотиците 2009-2013 г.;

5. Авторски колектив, "Наркотици, престъпления и наказания", Ефективни ли са мерките срещу наркоразпространението в България?, Български хелзинкски комитет, 2007 г.

6. Пазарът на наркотици в България, С., Център за изследване на демокрацията 2003 г.

7. Иван Владимиров, „Правен режим във връзка с наркотичните вещества", НБУ, Law Journal of NBU, 2011, N 1, www.nbu.bg /PUBLIC/IMAGES /File/.../7_ivan%20vladimirov.pdf

8. Организираната престъпност в България: пазари и тенденции, Център за изследване на демокрацията, 2007 г.

9. Годишен доклад по проблемите, свързани с наркотиците и наркоманиите в България, Република България, София, Декември 2013 г.

10. Нели Кирилова, доклад „Контрабанда в глобализиращия се свят. Рискове пред ЕС от новосъздаващите се демокрации. Място и роля на България", сборник на центъра за европейски и международни изследвания „Арабската пролет: надежда за промяна и предизвикателства пред Европейската външна политика и политика за сигурност, София, 2012 г.

КОНТРАБАНДАТА И НЕЗАКОННАТА ТЪРГОВИЯ С ОРЪЖИЕ И ЕФЕКТИВНАТА БОРБА С ТЯХ

Велико П. Петров

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "В. ЛЕВСКИ", ФАКУЛТЕТ "АРТИЛЕРИЯ, ПВО И КИС", КАТЕДРА "ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ТАКТИЧЕСКИТЕ ПОДРАЗДЕЛЕНИЯ ОТ ПОЛЕВАТА АРТИЛЕРИЯ" ГР. ШУМЕН

SMUGGLING AND ILLEGAL ARMS TRADING AND EFFICIENT COMBAT THEM

Veliko P. Petrov

ABSTRACT: *This report aims to acquaint the reader with smuggling and illegal trade in arms, which represent a profitable business for organized crime and have become a transnational phenomenon of paramount importance to modern society. The fight against these criminal acts require the combined efforts of all institutions working at national, regional and international level and covers a wide range of activities, including the management and security of stocks, transfer controls, maintenance of records destruction mechanisms for exchange of information and disarmament, demobilization and reintegration.*

KEYWORDS: *smuggling, illegal trade in arms*

Проблемът с незаконното разпространение на оръжия засяга не само Европа, а и засяга целия свят. Огнестрелни оръжия и резервните части и компоненти за тях се купуват все по-често онлайн и се доставят чрез каталози за поръчки по пощата, пощенски пратки или експресни куриерски услуги. Тези огнестрелни оръжия, когато попаднат в неподходящи ръце довеждат до унищожителни последствия за гражданите и обществото и от използване им се дават много жертви на насилие. Насилието, свързано с огнестрелни оръжия, продължава да причинява сериозни наранявания и загуба на човешки живот в целия Европейски съюз и е необходимо да се положат повече усилия за справяне с незаконния трафик на огнестрелни оръжия. Преразглеждането на действащото законодателство на Европейския съюз (ЕС) относно продажбата и прехвърлянето на огнестрелни оръжия в рамките на ЕС, в случай че бъде съчетано с по-сериозни практически усилия за правоприлагане, би намалило риска от незаконно използване и трафик на огнестрелни оръжия.

Злоупотребата с огнестрелни оръжия, независимо дали става въпрос за законно притежавани оръжия за граждански цели или за оръжия за граждански или военни цели, които са произведени или придобити по незаконен начин, представлява сериозна заплаха както за вътрешната, така и за външната сигурност на Европейския съюз.[1]

[1] Доклад на Съвета относно изпълнението на Европейската стратегия за сигурност – Гарантиране на сигурността в променящия се свят; „Стратегията за вътрешна сигурност на ЕС в действие: пет стъпки към една по-сигурна Европа" (COM (2010) 673)

С понятието „контрабанда" се обозначава всяко внасяне в страната или изнасяне на стоки в нарушение на местното законодателство. Контрабандата има международен характер, тя предполага нарушаване на митническия режим с пренасянето или превозването на стоки от една в друга страна през границите им. Контрабанда се извършва, за да се избегне заплащането на дължимите мита, данъци и такси, с цел да се постигнат финансови и търговски изгоди, като се избегне митническият, данъчният, полицейският и друг вид контрол и процедурите, свързани с регистрационни, разрешителни и лицензионни режими, заобикаляне на ограничения, свързани с вноса или износа на стоки и т.н.

В миналото (до 1989 г.) в Република България контрабандните канали са се наричали с термините „скрит транзит" или „скрита транзитна търговия" и с тях се обозначава държавно организираната вносна и износна контрабанда на стоки (оръжие, наркотици, алкохол, цигари, злато, сребро и всякакви луксозни стоки). Тази дейност се контролираше от Държавна сигурност и носеше десетки милиарди долари приходи. Преди монополизацията на скрития транзит от външнотърговското предприятие „Кинтекс" под шапката на Държавна сигурност, контрабанда в големи размери извършваха и други държавни предприятия – „Тексим", „Деспред" и „Разноизнос".

Ако до 1989 година контрабандните канали са необявена официална политика на еднопартийно контролираните тайни служби, то във времето на така наречения посткомунистически демократичен период незаконният трафик се е превърнал в хранилка на периодически сменящите се партийно-политически елити чрез посредничеството на сенчестия бизнес[2].

Контрабандата се счита за международно престъпление по силата на обичайното международно право. В българското законодателство контрабандата е уредена в чл. 242 от НК. Изпълнителното деяние на това престъпление се изразява в пренасяне на стоки през граница, без знанието и разрешението на митницата. С особено висока степен на обществена опасност е контрабандата на оръжие, наркотици и ядрен материал.

Незаконното производство, незаконният внос и продажбата на огнестрелни оръжия, представляват доходоносен бизнес за групите на организираната престъпност. Незаконно притежавани огнестрелни оръжия често се използват от организираната престъпност за принуждаване и сплашване на техните жертви. Много от огнестрелните оръжия, които се разпространяват незаконно, често са придобити чрез кражба или отклоняване от законосъобразното им предназначение, чрез нелегален внос от трети държави и чрез видоизменяне на други предмети в огнестрелни оръжия. В обществото в настоящия момент се поражда голямо безпокойство, което е в резултат на следните обстоятелства:

- дезактивирани огнестрелни оръжия незаконно се въвеждат отново в употреба и се продават с престъпна цел;

- изделия като сигнални пистолети, въздушни пушки и оръжия с халосни патрони се видоизменят в незаконни смъртоносни огнестрелни оръжия;

- престъпници могат да се възползват от технологиите за триизмерно печатане, за да сглобяват направени в домашни условия оръжия или да изработват компо-

[2] Кръстници на контрабандата в България, Откъс от книгата "Опус за българската контрабанда" на Петър Христозов, от 22.02.2008 г., http://afera.bg/siujeti/87.html

ненти, които се използват за повторното въвеждане в употреба на огнестрелните оръжия.

Търсенето на незаконни оръжия в България се определя от няколко фактора:

– нуждата на престъпния свят от такива оръжия – пистолети се търсят от всички криминално проявени, организираните престъпни групи използват сравнително по-често автомати „Калашников" или снайперски пушки;

– черният пазар – той е вторият стимул за нелегалната търговия и нелегалното производство на стрелкови оръжия и е създаден от престъпните групи в Западна Европа или в съседните страни. При това финансовият стимул на българските нелегални производители е особено силен, когато има чуждестранни клиенти.

– ловците търсещи евтини огнестрелни оръжия;

– неголямото търсене от граждани, които не са успели да получат разрешително.

Няколко различни източници снабдяват пазара на незаконни оръжия в Република България:

– *кражби от частни лица* – този източник на незаконно оръжие е ограничен, тъй като от 2004 г. кражбите на огнестрелно оръжие и взривни вещества се третират като престъпления с тежки последици, за които според Наказателния кодекс се предвижда лишаване от свобода за срок от една до десет години;

– *кражби от военни формирования* – този източник на незаконно оръжие е особено тежък по време на реформата във Въоръжените сили, когато големи количества малки оръжия и леко въоръжение са преместени в други военни бази. Най-често са крадени 9-мм пистолети "Макаров" и 7,62-мм автомати "Калашников" поради безотговорна отчетност на наличните оръжейни запаси;

– *кражби от военни заводи* – обикновено се заключава в кражба на части от произвежданите в съответния завод образци малки оръжия и леко въоръжение, а кражбата на цели оръжия е възможна на теория, но на практика се случва извънредно рядко;

– *нелегално производство и преправяне от бивши специалисти от предприятия на отбранителната или металургичната промишленост* – този източник е един от наложилите се източници за придобиване на незаконно оръжие, като в нелегалните цехове за производство оръжията се правят или от части, крадени от заводите или газови оръжия се преработват в огнестрелни. Най-често се среща в Старозагорския регион, особено в и около Казанлък, където се намира най-големият производител на малки оръжия и леко въоръжение, а именно компанията „Арсенал";

– *контрабанден внос от чужбина* – нерешените проблеми с граничната сигурност правят страната уязвима за контрабанда на редица стоки, между които и малки оръжия и леко въоръжение. Най-остър е проблемът със сигурността на самите гранични пунктове и с остарялото оборудване за граничен контрол. Най-тревожна е сигурността около летищата и пристанищата, а през тях преминава по-голямата част от износа на оръжие на страната. Това важи най-вече за Варна и Бургас (най-големите пристанища) от черноморска брегова ивица на България. Въпреки усилията на службите за граничен контрол, продължават опитите за контрабанда на малки количества малки оръжия и леко въоръжение през българските граници, като това обикновено става с превозни средства, преминаващи транзитно през страната, или е крайна дестинация на пратките (т. е. "внос"), или с превозни средства излизащи от страната (т.е. "износ").

Най-често срещаните примери за нелегален трафик на оръжия са:

- извършване на трансфер без лиценз;
- финансиране на забранен трансфер на оръжия;
- извършване на трансфер без запис за това какъв е той;
- фалшифициране на лиценз;
- притежание на незаконно оръжие, което после може да се продаде;
- опит за нарушение на стратегически търговски закон.

Наказанията, които държавите могат да налагат за незаконен трафик на оръжия варират от по-леки до по-тежки. Често срещани наказания са:
- предупредителни писма;
- глоби;
- отнемане на лицензи;
- отмяна на преференциални отношения;
- конфискация на предмети;
- затвор.

В епохата на глобализацията е безразсъдно държавите да останат с толкова различни законодателства, позволяващи развитието на такава опасна престъпна дейност. Разпространението на малките оръжия и лекото въоръжение се извършва чрез добре организирана мрежа, която достига всички краища на света. Така една държава формално може да не произвежда, внася или изнася отделни оръжия, но може да е част от международен път за черен трафик.[3]

Комисарят на ЕС в областта на вътрешните работи Сесилия Малмстрьом заяви „Незаконният трафик на огнестрелни оръжия представлява все по-голяма заплаха за сигурността на европейските граждани и е доходоносен бизнес за организираната престъпност. Трябва да засилим контрола на огнестрелните оръжия, които се движат в ЕС или го напускат, за да се предотврати злоупотребата с тях. Сключването на Протокола на ООН за огнестрелните оръжия потвърждава ангажимента на ЕС за защита на гражданите срещу риска от насилие, причинено с огнестрелни оръжия, както в ЕС, така и извън него".[4]

Европейския съюз търси балансиран подход, който е насочен към:
- регулиране на законното разпространение на огнестрелните оръжия за граждански цели (т.е. за невоенни цели) на вътрешния пазар;
- прекъсване на незаконното разпространение и употреба на огнестрелните оръжия за граждански цели;
- определяне на стандартите относно трансфера и посредничеството при конвенционалните бойни оръжия.

Международната конвенция на Организацията на обединените нации за борба с транснационалната организирана престъпност, приета на 15.11.2000 г., е първият инструмент в глобален мащаб за борба срещу транснационалната организирана престъпност и трафика с огнестрелни оръжия. Съществуват три протокола, които допълват Конвенцията, като в тях се предвиждат конкретни мерки за борба със специфични престъпления (трафика на хора, незаконния трафик на мигранти и незаконното производство и трафик с огнестрелни оръжия). Европейската общност

[3] Международно споразумение за търговията за оръжие – възможна алтернатива за решение на проблема с незаконния трафик

[4] Европейска комисия, съобщение за медиите, Брюксел, 22 март 2013 г. „Борбата с трафика на огнестрелни оръжия: Комисията предлага ратификация на протокола на ООН и по-нататъшни действия".

подписа Конвенцията и протоколите срещу трафика на мигранти и трафика на хора на 12.12.2000 г., а също и протокола срещу незаконното производство и трафик с огнестрелни оръжия на 16.01.2002 г.(неговото сключване се отложи в очакване на привеждането в съответствие на европейското законодателство). Протоколът има за цел предотвратяване, борба и ликвидиране на незаконното производство и трафика с огнестрелни оръжия, техните части и компоненти и боеприпаси. Той се обявява за наказване на производството и незаконния трафик с огнестрелни оръжия, техни части и компоненти и боеприпаси и на фалшифицирането или заличаването на маркировката на огнестрелните оръжия, и на опитите за подобно закононарушение или неговото улесняване в зависимост от различните правни традиции на държавите - страни по Протокола. Протоколът на ООН за огнестрелните оръжия, влезе в сила на 3 юли 2005 г.

В Държавен вестник брой 98 / 07.12.2005 г. е публикуван „Протокол срещу незаконното производство и трафик с огнестрелни оръжия, техни части и компоненти и боеприпаси към Конвенцията на Организацията на обединените нации срещу транснационалната организирана престъпност”[5], допълва Конвенцията на ООН срещу транснационалната организирана престъпност и следва да бъде тълкуван заедно с нея. В този Протокол в Чл. 3 са дадени следните термини:

а) „*огнестрелно оръжие*” е всяко преносимо оръжие с цев, което произвежда, предназначено е да произвежда или може лесно да бъде преработено така, че да произведе изстрел с куршум или снаряд чрез действието на експлозив, като се изключват антикварните оръжия или техни копия; антикварните оръжия и техните копия се определят в съответствие с националното право; в антикварните оръжия не се включват оръжия, произведени след 1899 г.;

б) „*части и компоненти*” означава всеки елемент или елемент за подмяна, конкретно предвиден за огнестрелно оръжие и от съществено значение за неговото функциониране, включително цев, тяло или цевна кутия, затворна рама или барабан, ударен механизъм или затворен блок и всяко устройство, което е предназначено или пригодено да заглушава звука от изстрела с огнестрелно оръжие;

в) „*боеприпаси*” са целият боеприпас или неговите компоненти, включително гилзи, възпламенители, заряд или куршуми, които се използват за огнестрелните оръжия при условие, че тези компоненти са под разрешителен режим в съответната държава - страна по протокола;

г) „*незаконно производство*” означава производство или сглобяване на огнестрелни оръжия, техни части и компоненти и боеприпаси: от части и компоненти, обект на незаконен трафик; без лиценз или разрешение от компетентен орган на държавата - страна по този протокол, където се извършва производството или сглобяването, или без огнестрелните оръжия да се маркират към момента на производството в съответствие с член 8 на протокола, лицензирането или разрешаването на производството на части и компоненти се извършва в съответствие с националното законодателство;

д) „*незаконен трафик*” означава вносът, износът, придобиването, продажбата, доставката, движението или трансферът на огнестрелни оръжия, техни части и

[5] „Протокол срещу незаконното производство и трафик с огнестрелни оръжия, техни части и компоненти и боеприпаси към Конвенцията на Организацията на обединените нации срещу транснационалната организирана престъпност”. Същият е издаден от МВР на Р. България и публикува в Държавен вестник брой 98 / 07.12.2005 г.

компоненти и боеприпаси от или през територията на една държава - страна по този протокол, към територията на друга държава - страна по този протокол, ако някоя от засегнатите държави не е дала разрешение за това в съответствие с разпоредбите на протокола или ако огнестрелните оръжия не са маркирани в съответствие, член 8 на този протокол;

е) „*проследяване*" означава систематичното следене на огнестрелните оръжия и където е възможно, на техни части и компоненти и боеприпаси от производителя до купувача, с цел подпомагане на компетентните органи на държавите - страни по протокола, при разкриването, разследването и анализа на незаконното производство и незаконния трафик.

На 15 - 16 декември 2005 г. Европейският съвет прие Стратегията на ЕС за борба с незаконното натрупване и трафика с малки оръжия и леки въоръжения (МОЛВ) и боеприпаси за тях (наричана по-нататък „Стратегия на ЕС за МОЛВ"). Стратегията на ЕС за МОЛВ определя подкрепата за Програмата за действие на ООН като първостепенен приоритет за действия на международно равнище и призовава за приемане на правно обвързващ международен инструмент за проследяване и маркиране на МОЛВ и боеприпаси.[6]

Европейският съюз прие през 2006 година Концепция на ЕС за подкрепа на разоръжаването, демобилизацията и реинтеграцията, която се съчета с усилията на Европейската Комисия и останалите европейски институции около Концепцията на европейската политика за сигурност и отбрана относно сектора за сигурност. Като приоритетни дейности са посочени основно мерките за борба с разпространението на леки стрелкови и малокалибрени оръжия.

Европол винаги е следил много отблизо развитието на този вид престъпност и неговите анализи позволяват да се хвърли светлина върху обхвата на незаконния трафик с огнестрелни оръжия в Европа. В няколко свои докладни записки Екипът за анализ и докладване на организираната престъпност на Европол (ОС - SCAN) вече предупреди държавите членки относно обхвата на незаконния трафик с оръжия и рисковете, свързани с него. През 2010 и 2012 г. бяха публикувани едно съобщение относно незаконния трафик и разпространението на тежки оръжия в рамките на Европейския съюз и едно ранно предупреждение относно „Автоматите Калашников - производство, търговия и незаконно използване в Европа". Извършеният от Европол (SOCTA) през 2013 г. анализ на заплахите, породени от тежката организирана престъпност, показва, че престъпните групировки използват трафика с оръжие като източник на доходи: 18 различни държави посочват 39 престъпни групи като извършващи трафик с огнестрелни оръжия или като основна дейност (25 групи) или като допълнителна дейност (14 групи).

Глобалната система за борба с разпространението на оръжия претърпя значително развитие след края на миналия и началото на настоящия век, като срещу разпространението на оръжия бяха издигнати солидни бариери. Експортният контрол е ключов инструмент в набора от инструменти за борба с разпространението на оръжия, но трябва да бъде винаги в крак с развитието на заплахите във връзка с разпространението на оръжия и с бързото технологично и научно развитие и про-

[6] „Решение на Съвета в подкрепа на дейностите на Службата на ООН по въпросите на разоръжаването в изпълнение на Програмата за действие на ООН за предотвратяване, борба и премахване на незаконната търговия с малки оръжия и леки въоръжения във всичките и аспекти" №12310/11, Съвет на Европейския съюз, Брюксел, 13 юли 2011 г.

мени в икономическата дейност в световен мащаб, които пораждат нови предизвикателства пред сигурността и се отразяват на равнопоставените условия на конкуренция на глобално равнище.[7]

ЕС предприема действия за установяване на слабите звена в кръговрата на огнестрелните оръжия и за търсене на възможности за преодоляването им, за защита на законното производство, продажба и притежаване на огнестрелни оръжия, за разбиване на веригите за доставки на черно и за ограничаване на незаконната употреба. Предприетите мерки на международно и национално равнище се съсредоточават върху следните няколко приоритета:

1) Защита на легалния пазар на огнестрелни оръжия за граждански цели посредством нови стандарти на ЕС, отнасящи се до това кои огнестрелни оръжия могат да бъдат продавани за граждански цели, каква маркировка следва да бъде нанасяна на огнестрелните оръжия и какви разрешения следва да се издават на лицата, желаещи да притежават и използват огнестрелни оръжия;

2) Ограничаване на отклоняването на огнестрелни оръжия към престъпните среди посредством изработването на ефективни стандарти относно безопасното съхранение на огнестрелни оръжия за граждански цели и относно начина на дезактивиране на огнестрелни оръжия за граждански и военни цели, както и чрез по-големи усилия за намаляване на незаконния трафик на огнестрелни оръжия (както за граждански, така и за военни цели), внасяни от страни извън ЕС;

3) Засилване на натиска върху пазарите на черно чрез подобряване на трансграничното сътрудничество между полицията, митниците и граничната охрана и чрез оценяване на необходимостта от общи правила на ЕС, отнасящи се до това кои свързани с огнестрелните оръжия деяния следва да бъдат квалифицирани като престъпления и какъв размер на наказателноправните санкции следва да налагат държавите членки;

4) Развиване и подобряване на разузнавателната дейност чрез събиране и обмен на повече сведения за свързаните с огнестрелни оръжия престъпления и чрез целенасочено обучение на служителите на правоприлагащите органи.

През периода 2011-2013 г. бяха отпуснати общо около 21 млн. евро от различни бюджетни редове на ЕС в подкрепа на разоръжаването, демобилизацията и реинтеграцията и за борба с незаконния трафик на огнестрелни оръжия, малки оръжия и леко въоръжение по целия свят.

През 2013 г. ЕС се присъедини към Протокола на ООН за огнестрелните оръжия[8], който ще спомогне да се затегне контрола върху трансфера на ръчни оръжия, пистолети и други малки оръжия при влизане и излизане от ЕС и на неговата територия.

В световен план приетият Договор за търговията с оръжие[9] (ДТО) ще доведе до нов етап в контрола на този вид търговия. Той задължава държавите, които са страни по него, да правят оценка на целия си износ с цел преустановяване на неза-

[7] Съобщение на комисията до Съвета и Европейския парламент, Преглед на политиката за експортен контрол: Гарантиране на сигурността и конкурентоспособността в един променящ се свят**,** Брюксел, 24.4.2014 г. COM(2014) 244 final, стр. 3.

[8] Протокол срещу незаконното производство и трафика с огнестрелни оръжия, техните части и компоненти и боеприпаси, допълващ Конвенцията на ООН срещу транснационалната организирана престъпност.

[9] Договорът за търговията с оръжие бе приет от Общото събрание на ООН на 2 април 2013 г.

конната търговия с оръжия и така да допринасят за мира и сигурността и да предотвратяват сериозните нарушения на международното хуманитарно право и международното право в областта на правата на човека.

Съгласно направения анализ на ДТО от компетентните български ведомства в практически аспект договорът не въвежда нови моменти в съществуващата добре развита национална система за експортен контрол. Прилаганите от Република България норми и стандарти в немалка степен надвишават заложените в договора. Договарянето на този инструмент беше сред приоритетите на страната ни и ЕС в областта на експортния контрол и политиката на търговия с оръжие.

Изводи:

1) Незаконното производство, незаконният внос и продажбата на огнестрелни оръжия, представляват доходоносен бизнес за групите на организираната престъпност и носят десетки милиарди долари печалба.

2) Изисква се ангажираност на всички държави към всестранен подход за насърчаване на местно, национално, подрегионално, регионално и глобално равнище и предприемане на действия за предотвратяване, борба и премахване на незаконната търговия с малки оръжия и леко въоръжение във всичките и аспекти. Тя обхваща широк кръг дейности, сред които управление и сигурност на запасите, контрол на трансфера, поддържане на регистри, унищожаване, механизми за обмен на информация и разоръжаване, демобилизация и реинтеграция.

3) Основен замисъл и приоритет на Договорът за търговията с оръжие е приносът към мира, сигурността и стабилността в международен и регионален план. Той е правно обвързващ инструмент, който, като установява високи общи международни стандарти за регулиране на международната търговия с конвенционални оръжия, цели да предотврати и да пресече нелегалната търговия и нерегламентираното отклоняване на конвенционални оръжия. ДТО е призван да запълни съществуващата празнота по отношение на регламентирането на международно равнище на търговията с конвенционално оръжие, като същевременно способства за укрепването на мира и хуманитарните дейности. Наред с това той увеличава прозрачността при търговията с оръжие, като насърчава воденето на отчетност и представянето на съответна информация.

4) Основната роля на Европол и в бъдеще ще е да предоставя подкрепа на правоприлагащите органи в ЕС, главно в усилията им да бъдат спрени и разбити опасните организирани престъпни и терористични групи. Този приоритет не е променен и няма да се промени, но правоприлагащите органи като цяло трябва да продължат да разработват нови политики, инструменти и тактики, за да са в крак със световните тенденции и да изпреварват престъпниците.

5) Необходимо е да се предприемат повече действия за установяване на слабите звена в кръговрата на огнестрелните оръжия и за търсене на възможности за преодоляването им, за защита на законното производство, продажба и притежаване на огнестрелни оръжия, за разбиване на веригите за доставки на черно и за ограничаване на незаконната употреба

Литература:

1. Доклад на Съвета относно изпълнението на Европейската стратегия за сигурност – Гарантиране на сигурността в променящия се свят; „Стратегията за вът-

решна сигурност на ЕС в действие: пет стъпки към една по-сигурна Европа“ (COM (2010) 673)

2. Кръстници на контрабандата в България, Откъс от книгата “Опус за българската контрабанда” на Петър Христозов, от 22.02.2008 г., http://afera.bg/siujeti/87.html

3. Международно споразумение за търговията за оръжие – възможна алтернатива за решение на проблема с незаконния трафик.

4. Европейска комисия, съобщение за медиите, Брюксел, 22 март 2013 г. „Борбата с трафика на огнестрелни оръжия: Комисията предлага ратификация на протокола на ООН и по-нататъшни действия”.

5. „Протокол срещу незаконното производство и трафик с огнестрелни оръжия, техни части и компоненти и боеприпаси към Конвенцията на Организацията на обединените нации срещу транснационалната организирана престъпност”. Същият е издаден от МВР на Р. България и публикува в Държавен вестник брой 98 / 07.12.2005 г.

6. Решение на Съвета в подкрепа на дейностите на Службата на ООН по въпросите на разоръжаването в изпълнение на Програмата за действие на ООН за предотвратяване, борба и премахване на незаконната търговия с малки оръжия и леки въоръжения във всичките и аспекти, №12310/11, Съвет на Европейския съюз, Брюксел, 13 юли 2011 г.

7. Съобщение на комисията до Съвета и Европейския парламент, Преглед на политиката за експортен контрол: Гарантиране на сигурността и конкурентоспособността в един променящ се свят, Брюксел, 24.4.2014 г. COM(2014) 244 final

8. Протокол срещу незаконното производство и трафика с огнестрелни оръжия, техните части и компоненти и боеприпаси, допълващ Конвенцията на ООН срещу транснационалната организирана престъпност.

9. Договор за търговията с оръжие, приет от Общото събрание на ООН на 2 април 2013 г.

10. Малки оръжия и леко въоръжение в България, Координационен център за контрол над малките оръжия и лекото въоръжение в Югоизточна Европа (SEESAC), 2005 г.

11. Светлозар Вешков, Оценка на съществуващата законова рамка в ЕС за борба с незакония трафик на оръжие.

12. Съобщение на комисията до съвета и Европейския парламент, Огнестрелните оръжия и вътрешната сигурност на ЕС: защита на гражданите и спиране на незаконния трафик, Брюксел, 21.10.2013 COM (2013) 716 final

13. Стратегия на ЕС за борба с незаконното натрупване и трафика на малки оръжия и леки въоръжения (МОЛВ) и боеприпаси за тях, документ на Съвета 5319/06.

14. Закон за ратифициране на Договора за търговия с оръжие, приет от 42-то Народно събрание на 12 март 2014 г., обнародван в ДВ бр.26 от 21 март 2014 г.

ЯВЛЕНИЕТО НЕЗАКОНЕН ТРАФИК НА ХОРА

Велико П. Петров

НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ "В. ЛЕВСКИ", ФАКУЛТЕТ "АРТИЛЕРИЯ, ПВО И КИС", КАТЕДРА "ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА ТАКТИЧЕСКИТЕ ПОДРАЗДЕЛЕНИЯ ОТ ПОЛЕВАТА АРТИЛЕРИЯ" ГР. ШУМЕН

PHENOMENON HUMAN TRAFFICKING

Veliko P. Petrov

ABSTRACT: *This report aims to acquaint the reader with traffic people who become a transnational phenomenon of paramount importance to modern society and therefore fighting it is difficult and less effective. The effects of this phenomenon led to consequences for individuals, political economies and implications for the legal system. Phenomenon requires the combined efforts of all institutions working at national, regional and international levels. Human trafficking is one of the eight priorities that Member States should address together.*

KEYWORDS: *phenomenon trafficking, illicit trafficking*

Трафикът на хора е световен проблем и засяга всички континенти и региони в света. Последните статистики сочат, че трафикът на хора засяга 4 милиона хора по света, измежду които от Източна Европа са около 300 000 жени. Незаконните приходи от този бизнес са оценени на няколко милиарда долара годишно според данни на Обединените Нации. Поставянето на ясно разграничение между миграцията, контрабандата (превеждането) и трафика на хора, на практика е изключително сложно и често невъзможно и това е така, понеже трите явления се преплитат и са част от движението на населението (идейно и функционално). Трите явления могат еднакво да се впишат като част от един динамичен сценарий във връзка с трансграничното движение на населението.

В продължение на много столетия, хиляди хора са ставали жертви на трафик за сексуални, трудови и други цели. Освен икономически причини, трафикът на хора, има дълбоки исторически, етнически и социални корени. Счита се, че трафика на хора е някаъв вид икономическа дейност или бизнес, в който участниците се стремят да извлекат печалба, а правната перспектива е тази дейност да се класифицира като престъпна. Така търговията с хора се разбира като нарушение на правните разпоредби на държавата и на отделните човешки права. Като изключително груба форма на икономическа престъпност, трафикът на хора е запазил основните си характеристики като престъпление през последните години:

– жертвите се набират от икономически по-изостанали страни и се транспортират в по-богати страни и региони, където живеят хора, готови да плащат в брой за предоставените им услуги;

– трафикът с цел принудителна проституция остава най-предпочитаната форма от трафикантите, поради простата причина, че им осигурява максимални печалби.

Трафикът на хора е съвременна форма на робство, тежко престъпление и сериозно нарушение на основните права на човека. По данни на Съвета на Европа (COE.int) трафикът на хора е третият най-голям източник на приходи за организираната престъпност и е най-бързо разрастващата се престъпна дейност в сравнение с други форми на организирана престъпност в ЕС.[1]

Трафикът на хора е организирана криминална дейност, която се провежда с цел за извличане на висока печалба чрез сексуална и трудова експлоатация на хора и е основна част от международната организирана престъпност. Печалбите от тази престъпна дейност могат да се сравняват само с тези от незаконна търговия с оръжие и наркотици. Криминалните групировки действат чрез насилие, заплахи и отнемане на личните документи на жертвите. Международната организирана престъпност се стреми да контролира все по-пълно трафика, демонстрира грубо нарушаване на човешките права на жертвите и оказва върху тях най-чудовищни форми на психологически и физически тормоз.

Явлението (от английската дума „trafficking“) се разбира едновременно като търговия с хора, оръжие и наркотици и незаконна търговия въобще. Използването на един и същ термин и за търговия с неодушевени предмети помага да се разбере една от страните на същността на феномена – че хора се третират като предмети. Общото понятие „трафик на хора“ включва съвкупност от обществено опасни деяния, насочени срещу личността и личната свобода в сферата на обществените отношения, свързани с основните права на човека на живот и свобода, включително с правото на личността да се разпорежда със собственото си тяло, с труда си и т.н.[2]

Според българското законодателство „трафик на хора” е набирането, транспортирането, прехвърлянето, укриването или приемането на хора, независимо от изразената от тях воля, чрез използване на принуда, отвличане, противозаконно лишаване от свобода, измама, злоупотреба с власт, злоупотреба с положение на зависимост или чрез даване, получаване или обещаване на облаги, за да се получи съгласието на лице, упражняващо контрол върху друго лице, когато се извършва с цел експлоатация.[3] От определението посочено в българския Закон за борба с трафика на хора (изготвено на основата на Протокола за трафика на хора, който допълва Конвенцията на ООН срещу транснационалната организирана престъпност) при разглеждането на трафика на хора се обособяват три взаимосвързани елемента:

– самият акт (какво е извършено) – набиране, транспортиране, преместване, укриване или приемане на хора;

– начинът (как е извършено) – със заплаха или със сила, с насилие или принуда, отвличане, измама или заблуда, злоупотреба с власт или уязвимост, заплащайки и давайки облаги на лице, което контролира жертвата/потърпевшото лице;

– целта (защо е извършено) – експлоатиране на проституирането на други лица, сексуална експлоатация, принудителен труд, заробване или подобни на робството практики или отнемане на телесни органи.

Трафикът може да бъде външен (извън границата на дадена държава) и вътрешен (в съответната държава). Вътрешен трафик е този, които се извършва в границите на страната, на нейната територия. Жертвите биват набирани от икономически по-изостанали райони и транспортирани към по-развитите части на страната. От

[1] Трафикът на хора продължава да расте, http://nasilie.eu/?p=3225

[2] Васил К. Миков, Автореферат на дисертация на тема „Проституция и трафик на хора с цел сексуална експлоатация в България: характеристики, причини, публични политики”, БАН, София 2013г. стр. 5.

[3] Закон за борба с трафика на хора, обн. ДВ, бр. 46 от 20.05.2003 г.

своя страна, международният трафик се осъществява чрез превеждане на жертвите през държавната граница и експлоатирането им в друга страна. Във връзка с това се говори по отношение жертвите на трафика на хора за:

– страни на произход – страните, от които се набират жертвите на трафик;

– страни на транзит – страните, през които биват транспортирани жертвите на трафик;

– страни на крайна дестинация – страните, в които жертвите биват експлоатирани.

България е източник, транзитен пункт и в малък процент крайна дестинация за Азия и Източна Европа. Стратегическото място, което заема България на Балканския полуостров и в Европа е причина нашата страна да има място в различните „канали на трафик на хора" и те са:

1) Русия – Украйна – Молдова – България – Гърция – Турция;

2) България – Молдова – Гърция – Албания – Италия;

3) България – Сърбия - Австрия – Германия – Белгия;

4) България – Сърбия - Австрия – Германия – Холандия.[4]

Причини за развитието на трафика на хора в България са:

– социално-културни – неграмотност, разпад на морални ценности, расизъм и етническа дискриминация, влияние на медиите и интернет;

– икономически – бедност, неразвита икономика, безработица;

– психологически – наркотична зависимост, психически и сексуален тормоз;

– геополитически – бежански потоци, международна организирана престъпност, географско положение[5].

Обекти на тази престъпна дейност могат да бъдат лица от различни възрастови, професионални и интелектуални групи. Трафикът на хора е организирана криминална дейност провеждана с цел получаване на високи печалби, като се използват различни форми на експлоатация: сексуална, трудова, просия, джебчийство, продажба на органи, продажба на новородени и други.

В каналите на трафик на хора може да попадне всеки човек. Има някои групи, които са особено застрашени и към които най-често е насочено вниманието на трафикантите:

1) **Децата** – те са голяма рискова група, тъй като те все още нямат натрупан социален и емоционален опит, не могат да разпознават рисковите ситуации и следователно могат да бъдат лесно манипулирани. Основни групи от деца, които биват въвлечени в трафик на хора са:

– деца от ромски произход, които са трафикирани в чужбина с цел джебчийство и просия;

– деца, отглеждани в Домовете за временно настаняване на деца, лишени от родителска грижа – най-често тези деца и юноши биват примамвани с обещания за по-добър живот в чужбина или в по-голям град в страната и там биват експлоатирани сексуално или трудово. Трафикантите се възползват от липсата на връзка със семейството на тези деца и нуждата им от близост и грижа. Много често трафикантите стават приятели на момичетата и така ги склоняват да работят за тях.

– деца на улицата;

[4] Кр. Захариева, Д. Георгиева, Трафик на хора - ниво на информираност на младите хора, научни трудове на Русенския Университет - 2011, том 50, серия 8.1, стр. 138

[5] Наръчник по превенция за трафик на хора, Национална комисия за борба с трафика на хора, септември, 2010 г., стр. 9.

– деца от проблемни семейства – това са деца, чиито родители нямат добра емоционална връзка с тях и не упражняват родителски контрол над тях. Подобни са и децата от семейства с домашно насилие. Проблемите в семейството ги карат да търсят разбиране и приемане на вън;

2) **Млади хора** – те се привличат най-вече чрез обещания за добре платена работа или обучение в чужбина като стават най-често жертви на сексуална експлоатация (вкл. млади мъже), както и на трудова експлоатация;

3) **Възрастни хора** – те са най-често хора, които са трайно безработни търсят възможности за работа в големите градове в страната или в чужбина. Те често се оказват принудени да работят при условия, близки до робските, при минимално заплащане и нехигиенни условия на живот и труд.

Най-голям процент от жертвите са принудени да работят в секс индустрията или порнографския бизнес. В своята същност трафика на хора нарушава основни човешки права като: право на живот и право на избор на свободен живот.

В процеса на осъществяване на престъпната дейност „трафик на хора" могат да бъдат разграничени *три етапа*:

1) Набиране на хора. В този етап средствата, които се използват включват заплаха, използване на сила, други форми на принуда, измама, подвеждане, заблуда, злоупотреба с власт или с уязвимост, заплащане или получаване на някакви други изгоди от лицето, което контролира жертвата. Най-често се използва *измамата,* като трафикантите дават обещания за високоплатена работа, женитба, подобър живот, пари, материално благополучие и придобивки. Най-лесно биват измамени хора, които са уязвими – млади хора, избягали от дома, живеещи на улицата, бедни, хора с проблеми в семействата. За да постигнат успех трафикантите се опитват да се сприятелят с потенциалната жертва, а понякога дори се преструват, че са влюбени в тях. Ако създаването на по-близки отношения се окаже безуспешно, трафикантите прибягват до отвличане, а също могат да използват и физическо насилие, заплахи или други форми на принуда.

2) Транспортиране (превозване). Този етап също може да бъде принудителен – ако жертвата е била отвлечена или заплашена. Трафикантите преместват жертвите далече от дома им, за да могат по-лесно да ги контролират. Ограничават свободата им, като им конфискуват документите и ги правят зависими. Когато трафикът е външен, трафикантите транспортират жертвите в чужда страна, където обичайно жертвите не познават никого, не познават езика и културата. Понякога използват фалшиви документи. В повечето случаи жертвите биват препродавани многократно преди достигане на крайната дестинация, нерядко биват изнасилвани.

3) Експлоатация на хора. Това включва като минимум сексуална експлоатация, включително чрез проституция, чрез принудителен труд, робство, слугуване или отнемане на човешки органи от жертвите. Жертвите на трафик, тотално загубват контрола върху живота си, което се случва чрез използването на система от психологическо, физическо и сексуално насилие върху тях. Трафикираните биват измамени и експлоатирани, като се злоупотребява с тях и често живеят в робски условия. Дори тези, които решават да мигрират, за да работят, често не знаят или са били заблудени за условията, при които ще трябва да работят. Трудовите условия са тежки, не се спазват изискванията за безопасност, заплащането е много ниско и сериозно се различава от първоначално договореното, то бива забавяно и използвано за изнудване на работещите, често е налице и сексуален тормоз. Работят дълги часове, отнети са правата им на почивка и медицински грижи, не могат да разчитат и на грижата и

защитата на семействата си. Много жени и девойки се оказват в ситуация на експлоатация, при която са принудени да работят против волята си - например като домашни помощнички, в цехове, във фабрики, в секс-индустрията и други. Те биват подложени на различни форми на злоупотреба и насилие и загубват контрола върху живота си. Някои от жените и децата биват принуждавани да работят в секс индустрията, а други - в организираната просия, като прислужници в частни домове, в шивашката, в риболовната, в минната и други индустрии, във ферми и плантации, като често биват въвличани и в престъпни дейности.

Има склонност към отъждествяване на понятието „трафик на хора“ с проституцията. По определение проституцията е дейност, извършвана от дадено лице за задоволяване сексуалните потребности на друго лице срещу някакво възнаграждение, като лицето съзнава какво върши и има за цел да го върши, тоест такава е неговата воля. По своя воля лицето може да приеме или да откаже предоставянето на услугата и то само получава и ползва уговореното възнаграждение. Само решава кога да практикува и кога не и то решава кога да прекрати дейността си. Разбира се, съществуват и форми на организирана проституция, но и при нея също се прилага принципът на договарянето за съвместна дейност.

За разлика от проституцията, при трафика на хора нещата не стоят така. При въвличане в трафик жертвата не действа по своя воля, тя е заставена да изпълнява чужда воля. Тя не може да откаже извършването на услугата, а възнаграждението се получава и ползва от трафикантите. Жертвата не решава сама кога да практикува – тя е насилвана да го прави непрекъснато. Всичко това не е в нейна власт да прекрати дейността си, да се „откаже“.

Въпреки че търговията с човешки органи се преследва от законите в целия свят с изключение на Китай и Иран, в редица развиващи се страни те са „стока“. Най-често продавани са бъбреците, защото са два и при операция без усложнения човек може да живее и с един бъбрек. В Турция този орган се продава между 2500 и 5000 долара, а в Пакистан - около 1000 долара. За да се сдобие със „стоката“ обаче, нуждаещият се от бъбречна трансплантация заплаща между 150 000 и 200 000 долара в клиника в Израел или между 50 000 и 100 000 долара в Русия. Другите органи - като сърце или черен дроб, се набавят предимно от трупен донор (освен случаите, когато част от черния дроб на родителя се присажда на бебето). За това често се продават живи деца, от които се извличат „резервните части“. Присаждането на сърце струва около 80 000-100 000 долара, а на черен дроб - близо 200 000 долара. Предполага се обаче, че живите деца са продавани за не повече от 10 000 долара. Схемата за трафик на органи е организирана както при всички контрабандни стоки. Тук обаче съществува нюансът на доброволно донорство. В този случай има замесени лекари, които вербуват жертвата с обещание за пари и по-добър живот без здравословни усложнения. Най-податливи на това са бедните, отчаяни или безработни хора[6].

Правата на жертвите са анализирани от гледна точка на минималните стандарти, включени в Протокола за предотвратяване, потискане и наказване на трафика на хора, особено на жени и деца, към Конвенцията на ООН за борба с международната организирана престъпност (Палермо протокола), Конвенцията на Съвета на Европа за борба с трафика на хора, Директива на Европейския съюз 2011/36/ЕС за предотвратяване и борба с трафика на хора и защита на жертвите му и други меж-

[6] Мариана Тодорова, Трафикът на човешки органи, http://www.temanews.com /index.php?p=tema&iid=446&aid=10396

дународни документи. На българско ниво тези права са предвидени в следните основни закони:

• Наказателно-процесуалния кодекс (НПК);

• Закона за борба с трафика на хора;

• Закона за социалното подпомагане;

• Закона за подпомагане и финансова компенсация на пострадали от престъпления (Закона за подпомагане и компенсация).[7]

Жертвите все по-добре познават правата си и могат да изискват намесата на съдебните власти, да се обединяват в групи и да търсят съдействие от правни консултанти. Като цяло, те познават правата си точно както ги познават и обвиняемите – за разлика от положението в миналото – и са готови да ги отстояват. Жертвите са човешки същества, които искат защита, да бъдат изслушани или да получат обезщетение за отрицателните последици на правонарушението, от което са пострадали. Всяка жертва е преди всичко носител на конкретни права, а това следва да се признава чрез осигуряването на набор от мерки, предвидени не само в наказателното право[8].

Така, в глобален план, а оттам и на българско ниво, бе „преоткрита" ролята на пострадалите и бе подновено вниманието, което им се отделя. Появата на жертвите на правната и политическа сцена през последните години бе обусловено и от един друг фактор: увеличилият се брой престъпления доведе и води до все по-голям брой хора, които в наше време са изложени на риска да се превърнат в жертви. В България жертвите на престъпления получиха дължимото внимание от органите, формиращи наказателната политика и законодателя. През последните години множество правителствени актове - стратегии, концепции и т.н. подчертаваха необходимостта от специални мерки в тази област. Наказателно-процесуалният кодекс от 2005 г. за пръв път уреди процесуалното положение на пострадалия. Жертвите вече имаха правата на частен обвинител, частен тъжител и граждански ищец. Сега те станаха титуляри на допълнителни права. През 2006 г. бе приет Закон за подпомагане и финансова компенсация на пострадали от престъпления, който допълнително призна и гарантира правата и законните интереси на жертвите. Освен различните видове подкрепа (психологическа, правна, медицинска и т. н.) предвидена е ограничена финансова компенсация от страна на държавата. В допълнение, някои нови законодателни актове предвидиха защита и подкрепа на отделни видове жертви - на домашно насилие, трафик на хора и др.

Изводи:

1. С глобализацията на престъпността трафикът на хора се превърна в транснационален феномен от изключително значение за съвременното общество, поради това борбата с трафика е трудна и малко ефективна. Законодателят и съдебната власт не могат да разпознаят с точност явлението, което обществото като цяло не вижда ясно. Поради това ефективното противодействие срещу трафика започва от

[7] Наташа Добрева, Защита на правата на пострадали от трафик на хора в България, Подход, основан на международната регулация на правата на човека, Изследването е по проект „Подпомагане на правото на жертвите на трафик в България, Словакия и Румъния да получават правна помощ - подход, основан на правата на човека" (HOME/2011/ISEC/AG/4000002581), стр.10.

[8] Добринка Чанкова, "Развитие на политиките, свързани с жертвите на престъпността в България в последно време", доклада е представен на 13-ти международен симпозиум по виктимология, Мито, Япония, 23-28 август 2009г., стр. 2

усилието обществото да осигури съдържателна равнопоставеност на своите членове, тъй като в нея се намират алтернативите на престъпната експлоатация.

2. Въздействията на явлението „трафик на хора" довеждат до:

1) Последствия за отделните лица – лицата (жертвите) на трафика на хора, изпитват престъпното му въздействие във всички области на живота си и се сблъскват с физическо, сексуално и психологическо насилие, принуждаване към употреба на наркотични вещества, извършване на престъпления, с икономическа експлоатация и тежки условия на живот и труд. Като насилствено престъпление трафикът на хора причинява физически и психически травми, чийто последствия са с дълготраен ефект и въздействие;

2) Политически последствия – това явление създава сложни взаимовръзки между политиката и практическите действия на държавата за недопускането му. Свързано е с транснационалното преместване на хора и създава проблеми в областта на миграцията, на трудовата заетост, в икономиката и социалната дейност. Поражда се необходимост от ангажиране на международната общност за съвместни действия и политики, да се разработват документи, в които да се идентифицират някои от най-значимите социални, политически и икономически въздействия на явлението и се очертаят важните политически възгледи във всяка от тези области;

3) Последствия върху икономиката – често е невъзможно да се изчислят. Явлението намалява човешките ресурси, съкращава финансовите ресурси и пряко засяга икономиката на държавата. Престъпните доходи са значителни, имат глобален характер и са постоянен източник за финансиране на организираната престъпност;

4) Последствия върху правната система – трафикът на хора нарушава правовия ред, засяга националната и международната правна система и е ефективен механизъм за незаконно преразпределяне на национално богатство като въздейства негативно на отношенията в политическата и социална сфера. Засяга се финансовата система, икономиката и социалната структура на страните и има сложно взаимосвързано негативно въздействие във всичките области на политическия, социалния, икономическия и правния живот на отделната държава.

3. Транснационалният характер на явлението изисква обединените усилия на всички ангажирани с проблема институции на национално, регионално и международно ниво. В Приетата през юни 2012 г. Стратегия на ЕС за изкореняването на трафика на хора за периода 2012—2016 г. е съсредоточена върху по-активното съдебно преследване на трафикантите на хора, оказването на помощ и защита за жертвите на трафика и предотвратяването на трафика на хора. Трафикът на хора е един от осемте приоритета, с които държавите членки на ЕС следва да се справят заедно, за което беше разработена специална методология (Цикъл на политиката на ЕС за борба с организираната и тежката международна престъпност) с ясни цели, конкретно прилагане и изисквания към последващите действия.

ЛИТЕРАТУРА:

1. Васил К. Миков, Автореферат на дисертация на тема „Проституция и трафик на хора с цел сексуална експлоатация в България: характеристики, причини, публични политики", БАН, София 2013г. стр. 5.

2. Закон за борба с трафика на хора , обн. ДВ, бр. 46 от 20.05.2003 г.

3. Национална програма за предотвратяване и противодействие на трафика на хора и закрила на жертвите за 2009 г.

4. Белова, Г., Н. Марин, С. Паслар и Й. Кочев. „Международноправни аспекти на трафика на хора". Асоциация на прокурорите в България Бюлетин №3, 2010, с.53.

5. Наташа Добрева, Защита на правата на пострадали от трафик на хора в България, Подход, основан на международната регулация на правата на човека, Изследването е по проект „Подпомагане на правото на жертвите на трафик в България, Словакия и Румъния да получават правна помощ - подход, основан на правата на човека" (HOME/2011/ISEC/AG/4000002581);

6. Тоше Благой Панов, Автореферат на дисертация на тема ”Трафикът на хора според законодателствата на Република България и Република Македония”, ЮЗУ „Неофит Рилски”, Благоевград, 2014 г.

7. Кр. Захариева, Д. Георгиева, Трафик на хора - ниво на информираност на младите хора, научни трудове на Русенския Университет - 2011, том 50, серия 8.1, стр. 138.

8. Наръчник по превенция за трафик на хора, Национална комисия за борба с трафика на хора, септември, 2010 г.

9. Стратегия на ЕС за изкореняването на трафика на хора за периода 2012-2016 г.

10. Мариана Тодорова, Трафикът на човешки органи, http://www.temanews.com / index.php?p=tema&iid=446&aid=10396

11. Добринка Чанкова, ”Развитие на политиките, свързани с жертвите на престъпността в България в последно време”, доклада е представен на 13-ти международен симпозиум по виктимология, Мито, Япония, 23-28 август 2009г.

12. Камен Пенков, Трафикът на хора – форми на проява и противодействие.

ВЪЗНИКВАНЕ И РАЗВИТИЕ НА ОНЛАЙН РЕКЛАМАТА КАТО ЕЛЕМЕНТ НА МАРКЕТИНГА

Светослав Р. Велков
УНИБИТ

Адрес за кореспонденция: 1463 София, ул. „Тунджа” 23, ап. 5

EMERGENCE AND DEVELOPMENT OF ONLINE ADVERTISING AS AN ELEMENT OF MARKETING

Svetoslav R. Velkov

***ABSTRACT**: The prerequisites for the emergence and development of the online advertising are presented. Its advantages and disadvantages as an effective tool of marketing, which is significantly different from traditional marketing tools and gives rise to more interest with increasing importance of the internet as a means of information and communication.*

***KEY WORDS**: Internet, online advertising, marketing*

Темата, занимаваща се с проблемите на онлайн рекламата в световната мрежа, буди все по-голям интерес с нарастване на значението на интернет като средство за

информация и комуникация. Самият факт, че мрежата вече е навлязла в почти всички страни и региони на земното кълбо, дава достатъчно основание да се смята, че това е проблем от голямо обществено и икономическо значение.

Макар и толкова значими, проблемите на интернет рекламата не са обхванати цялостно от професионалната литература. Това се дължи до известна степен на факта, че тази област от съвременната маркетингова наука е сравнително нова и на това, че тя не престава да се развива. От друга страна обаче, се наблюдава и известно подценяване на значението на интернет комуникацията като маркетингов елемент и обръщане на практиците и теоретиците към по-познати и утвърдени сфери на маркетинга и рекламата. С голяма убеденост може да се твърди, че това е резултат и от непознаването на онлайн бизнеса, но неговото сигурно позициониране в публичната среда принуждава специалистите, които се занимават с маркетинг, категорично да го припознават като съществен маркетингов елемент. Също така е вярно, че много малко неща свързани с онлайн рекламата могат да бъдат наречени класика. Фактът, че формите на рекламата в интернет са толкова разнообразни и се променят с високи темпове прави материята трудна за класификация и обхващане в корпуса на научната маркетингова мисъл.

Важно значение за избора на темата на доклада за мен имаше именно фактът, че интернет е комуникационно и информационно средство с възможности по-големи от възможностите на всички останали видове медии, които се използват в наши дни. От тази гледна точка въпросът за това, защо рекламата не може да се възползва напълно от тази уникална медия изглежда още по-интересен. Като илюстрация на това колко привлекателен и нов е светът на онлайн рекламата искам да използвам знаменитата фраза на американския милиардер Пол Гети, който казва: „Знам, че най-малко половината от моите рекламни долари се изразходват напразно. Не знам само коя половина”[1]. В света на интернет и това е известно.

В наши дни интернет е вездесъщ и много от нас не си представят съвременния свят без него. За първи път в историята на човечеството чрез интернет може да се комуникира толкова бързо, масово и глобално. С възможността си да ангажира аудиторията с най-интерактивни и иновативни методи, без „работно време” и навсякъде по света, интернет и онлайн маркетингът имат нужда от нов съвременен подход и осмисляне. От гледна точка на маркетинга интернет набира все по-голямо значение и вече се е изравнил по важност с такива утвърдени канали на маркетинговата комуникация като телевизията и печата. Многообразието на формите и средствата, голямата свобода на избора, съчетани с ефективност и гъвкавост дават възможност интернет да се използва като медия, като канал за директен маркетинг и като средство за дистрибуция. За този процес спомагат и предимствата, които има интернет пред традиционните средства за реклама:

- интернет е ефективно средство за представяне на рекламирания обект. Това е свързано от една страна, с възможностите за предоставяна на максимума необходима информация за това, което рекламираме и от друга с мултимедийната същност на неговата среда, която позволява да си използват всички възможни начини за въздействие върху потребителя, а именно текст, графика, звук, видео. Освен това, хипертекстовите свойства на мрежата дават възможност на потребителя сам

[1] Огилви Д., Изповедите на един рекламист, Princeps, С., 1999, с. 159.

да контролира търсенето и получаването на информация и по този начин го въвлича по-пълно в комуникационния процес;

- интернет е интерактивна среда, в която рекламата може да въздейства не само пасивно, но и активно върху своите адресати;

- интернет предоставя възможност на рекламодателя да фокусира много точно своята реклама върху целевата аудитория;

- относително ниската цена на изработването на различните форми и краткото време за публикуването им в интернет, позволяват завидна гъвкавост и динамика при протичането на една рекламна кампания онлайн, както и промяна на тактиката на рекламната кампания при необходимост;

- нещо уникално за интернет средата, което не откриваме в никоя друга медия е измеримостта, като данните се следят в реално време с точност до един потребител;

- бързината на организацията и реализацията на онлайн кампаниите в интернет, без това да е за сметка на качеството, е най-доброто решение за кризисни или други спешни ситуации, в които е необходима незабавна реакция;

- интернет дава възможност за прецизно планиране на честотата на излъчване (frecuency) до един реципиент, като позволява една кампания да се оптимизира добре и да се избегнат нежеланите реакции, като пренасищане например;

- тъй като се базира на модерни технологии, интернет предоставя невиждани до сега възможности за оперативен и дълбок анализ на проведените рекламни мероприятия.

Тези предимства създават предпоставките интернет маркетингът да се използва за:

- позициониране, динамизиране и модернизиране на имиджа на марката (чрез онлайн кампания, оригинален сайт, сайт за услуги или брендирана секция);

- осъществяването на поддържащи кампании при анонсирането на нов продукт (с помощта на банери-тизъри, интерактивни кампании и текстови съобщения);

- достигане до специфична аудитория, набиране на нови клиенти, маркетингови проучвания, изграждане на лоялни групи; създаване на нови канали за продажба (чрез подготовка за покупка, препоръка на приятел, публикувани статии, съобщения, онлайн каталози или електронни магазини).

В този контекст изказването на Рич Стюарт, маркетинг мениджър на Ford, който като споделя опита си след мащабна онлайн рекламна кампания на F-150 през 2004 г. отбелязва, че онлайн е най-ефективната в ценово отношение медия и представлява много привлекателна възможност за развитие е достатъчно показателно.

Същевременно интернет, като инструмент на маркетинга и рекламата, значително се различава от традиционните маркетингови средства, затова за по-доброто разбиране на маркетинговите комуникационни функции на световната мрежа е необходимо да се запознаем с възникването и да проследим развитието на интернет и онлайн рекламата в исторически план.

Да се открие началото на една мрежа е трудна задача, защото мрежата се състои от звена, а колко от тези звена са необходими , за да има мрежа? Някои определения посочват че свързаните един с друг средства или хора трябва да са най-малко две/двама за да има мрежа.

В съответствие с това по какъв начин разбираме понятието мрежа ние можем да разглеждаме създаването на интернет, като доста продължителен процес. За

официална начална година на онлайн летоброенето се смята обаче 1969 г., когато четири големи компютъра на университетите UCLA, Stanford Research Institute, UCSB и University of Utah са свързани в APRANET (Advanced Research Projects Agency NET).

Разработена първоначално за военни цели и след това намерила топъл прием в академичните среди APRANET се разраства с геометрична прогресия по отношение на броя на включените в нея звена. В същото време мрежата започва бавно и постепенно да придобива днешните си свойства и характеристики. През 1972-а се появяват e-mail и протоколът telnet, а през 1973 г. е въведен и ftp протоколът, който позволява обмяна на файлове през мрежата.

Паралелно с APRANET, но независимо от нея се развива и мрежата свързваща електронните каталози на множество библиотеки в САЩ. По-късно тези ресурси стават достъпни до по-широка общественост с помощта на протоколът telnet.

Следващата голяма стъпка в развитието на мрежата става факт през 1983 г. когато е въведен за масово използване протоколът TCP/IP, който се използва и до днес като основен при осъществяването на връзка между компютрите.

През 1986 г. американската National Science Foundation създава NSFNet, която представлява комуникационна инфраструктура, способна да предава информация със скорост от 56 Kbps и успява в продължение на следващото десетилетие да субсидира безплатното й използване за правителствени и изследователски цели.

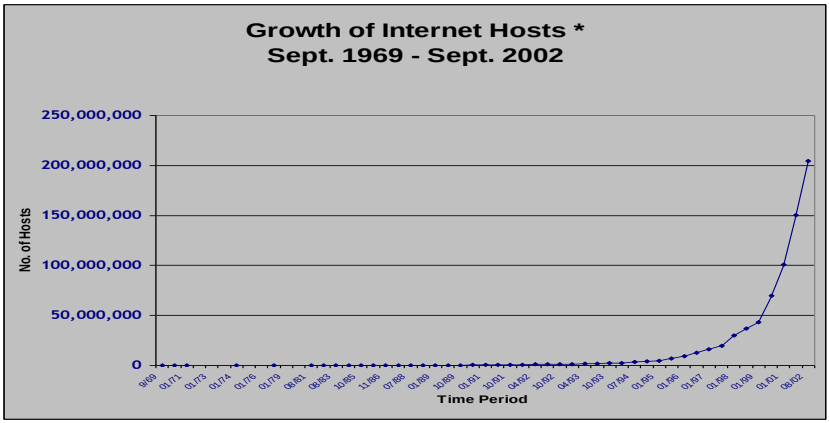
До този момент използването на мрежата е било сложно и хората, които са искали да работят с нейните ресурси е трябвало да се подготвят специално за това. Не е съществувал нито съвременния графичен интерфейс, нито интернет страницата. Необходими са били специални умения за да се прочете дори един e-mail. Това заедно с факта, че персоналните компютри не са били нито толкова разпространени, нито толкова мощни, за да се включат в мрежата определя и характера на ранния Интернет. Той е бил в истинския смисъл на думата некомерсиализиран, а ползващите го са били държавни и университетски служители. Затова на този етап на развитие, в мрежата все още няма никакви форми на рекламни съобщения.

Интернет започва да се развива истински скоростно едва през 90-те години на миналия век. Основният фактор за това е въвеждането на стандартите URL и HTML. Това е може би едно от най-важните събития в историята на интернет от гледна точка на бизнеса, защото полага основите за създаване на World Wide Web. Възникването на World Wide Web се свързва с името на Tim Bernes Lee (по онова време служител на CERN в Швейцария), който още през 1989 г. разработва World Wide Web като интернет базирана хипермедийна инициатива за обмяна на информация в глобален мащаб. С помощта на езика за разполагане на хипертекст (Hypertext Markup Language, HTML), който представлява набор от инструкции за форматирането на документи, световната мрежа свързва и унифицира огромна част от информацията, намираща се в интернет под формата на текст, звук или картина.

През 1990 г. Tim Bernes Lee написва и първите програми за уеб клиент (наричан днес браузър) и за уеб сървър. Това прави възможно през 1991 г. да се появи първата уеб страница, която е на Stanford Linear Accelerator Center. В същото време започва и изграждането на множество независими частни мрежи, които не са били подвластни на ограниченията на правителствено субсидирания интернет. Когато независимите мрежи се свързват по между си става възможно трафикът на информация изцяло да заобикаля правителствената инфраструктура NSFNet. През 1995 г.

се прекратява правителственото субсидиране на NSFNet, а с това отпадат и всички ограничения за търговското използване на интернет. От този момент нататък трафикът на данни се поема изцяло от комерсиални инфраструктури.

Изключително добра представа за темповете на развитие на глобалната мрежа дава Фигура 1, показваща броя на интернет хостовете[2] от септември 1969 г. до същия месец на 2002 г.



Фигура 1.

Източник: Internet Society, Internet History and Growth, by William Slater III - Chicago Chapter of the Internet Society, http://www.isoc.org/internet/history/

През 2000 г. интернет има вече 407 милиона потребители в 218 от 246 страни по света, а само 2 години по-късно потребителите на интернет са вече двойно повече – през 2002 г. в интернет има вече 840 милиона потребители[3]. Понастоящем[4] само в Google Plus вече има над 195 милиона регистрирани потребители, което не е никак малко, но имайки предвид, че Twitter има 140 милиона, а Facebook сигурно вече минава 900 милиона потребители, а по данни на *pingdom*[5] броят на потребителите на Интернет е 2,1 млрд. души.

При това развитие на събитията не закъснява и първата реклама в интернет пространството. На 12 април 1994 г. Лорънс Кантер и Марта Сийгъл разпращат първи масов e-mail, промоциращ адвокатската им кантора в САЩ. В същата година, но през октомври HotWired публикуват и първите рекламни банери, рекламиращи бира. Сред първите рекламодатели се нареждат AT&T, MCI, Sprint и Volvo.

[2] Интернет не е бил известен като „Интернет" до януари 1984 г., когато е имало вече 1000 хоста, които са били настроени за използване на TCP/IP протокола.

[3] Източник: Internet Society, Internet History and Growth, by William Slater III - Chicago Chapter of the Internet Society, http://www.isoc.org/internet/history/

[4] http://newtrend.bg/social-media/ekskluzivno-kolko-sa-registriranite-potrebiteli-na-google-plus-195-miliona

[5] http://bg.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82

През следващите няколко години рекламата в интернет започва да се развива все по-бързо и по-бързо. Средствата похарчени за реклама през 1995 г. достигат 37 милиона долара, а интернет потребителите набройват вече 5 милиона. През следващата 1996 г. разходите за интернет реклама се увеличават с близо 800% и достигат 301 милиона долара, а парите похарчени за интернет пазаруване – 1,3 милиарда долара. Появяват се и първите анимирани банери. Също тогава на пазара навлиза и рекламното оформление на интернет страниците – т.нар. брендинг сайтове.

Развитието на банерната реклама в интернет е толкова бурно, че още през 1996 г. Coalition for Advertising Supported Information and Entertainment (CASIE) предлага и първите правила за стандартизиране на банерните рекламни съобщения. Паралелно с това започват да се оформят маркетинговите стратегии в електронното пространство. Един от първите белези за това е появата на разнообразни начини за определяне на цената на рекламата в интернет. Маркетинговите специалисти са принудени да са гъвкави, защото работят в една изключително динамична среда във всяко едно отношение. Както и в самото начало на комерсиалното използване на мрежата, така и днес рекламата в Интернет се развива под въздействието на три взаимно свързани и догонващи се фактори. Това са техническият прогрес, маркетинговата мисъл и физическото разрастване на интернет. Те образуват система от три неразривно обвързани точки, които са движещата сила на рекламата:

- техническият прогрес е изключително важен фактор. Техническите нововъведения могат да променят характера на глобалната мрежа много бързо. Могат да я направят по-високо скоростна, по-надеждна, по-евтина и по достъпна, но също така могат да открият и нови възможности за използването на интернет за комерсиални цели, от което се възползва маркетинговата мисъл;

- маркетинговата мисъл, от своя страна, също е в състояние да направи мрежата по-привлекателна за потребителите или пък по-достъпна за тях в ценово отношение. Намирайки нови методи за реклама и комуникация с клиентите маркетинговата мисъл прави интернет още по-привлекателен за бизнес потребителите. От друга страна, маркетинговата мисъл въздейства и върху техническия прогрес, превръщайки самата интернет инфраструктура в динамичен и доходоносен бизнес (част от телекомуникационния бизнес), в който се вливат значителни средства за научноизследователска дейност;

- физическото разрастване на интернет се изразява в разпространението му до все повече точки на планетата и въздейства както върху необходимостта от технически прогрес, така също върху маркетинговата мисъл. Със своето разрастване (разпространение) глобалната мрежа придобива все по-голямо значение и стимулира другите два фактора, които на свой ред влияят върху нейното развитие.

И трите фактора са взаимно свързани и е трудно да се определи, кой от тях дава първоначален тласък за развитието на останалите. За да се разберат принципите на онлайн рекламата обаче трябва вземем за наша отправна точка маркетинговата мисъл, но да не изпускаме от вниманието си и да разглеждаме внимателно и трите фактора. Това е необходимо, защото както вече подчертахме, маркетинговата мисъл получава входящи импулси от другите два фактора и произвежда изходящи импулси към тях.

Когато разглеждаме досегашното развитие на онлайн рекламата е добре да се съобразяваме със системата от трите фактора по две причини:

Първо, така можем да систематизираме появата на даден тип реклама в интернет.

И второ, изучавайки вече протеклите процеси да направим по-верни предположения за бъдещето развитие в тази област.

И така, първият исторически възникнал тип онлайн реклама е рекламното съобщение изпратено чрез системата за електронна поща. Предпоставка за осъществяването на тази реклама е техническият прогрес, направил възможно изпращането на имейл, който от своя страна е бил резултат от физическото разпространение на интернет. В момента, в който ползвателите на интернет са надвишили един критичен брой и обменяната помежду им информация се е увеличила дотолкова, че да не може да бъде обработена в момента на изпращането й (съответно получаването й), се е появила необходимостта от създаването на електронни пощенски кутии, които да съдържат съобщенията за тяхното първоначално и последващо използване. В този случай не е било трудно маркетинговата мисъл да направи паралел, да установи сходството между традиционната поща и тази в електронното пространство и да се възползва от новосъздадения канал за комуникация.

При разгледания тип реклама ясно се вижда линията и последователността на взаимодействие между трите фактора. Физическото разпространение въздейства върху необходимостта от научно-техническа новост, от което се възползва маркетинговата мисъл. Този начин на протичане на процеса не е универсален. Иницииращият и резултиращият фактор може да бъде всеки един от трите.

При банерите, които представляват вторият исторически възникнал тип онлайн реклама можем да проследим по-различно протичане на процеса на взаимодействие между трите фактора. А именно - научно-техническите новости URL и HTML, позволяват да се създадат първите интернет страници с опростен за ползване графичен интерфейс; той от своя страна дава възможност на по-голям брой потребители (включително и такива без специални познания в областта на PC и интернет) да ползват мрежата, а от това в крайна сметка се възползва маркетинговата мисъл, която създава графични рекламни послания и ги разполага върху посещаваните интернет страници.

Третият, по хронологичен ред, вид онлайн реклама в лицето на брендинговите и спонсорираните интернет страници имат за иницииращ фактор маркетинговата мисъл, а за резултиращ – физическото разпространение на интернет. Като се възползва от наличните технически възможности маркетинговата мисъл създава условия, в които бизнесът работи за потребителите на интернет, създавайки нови интернет страници и предоставяйки нови безплатни информационни ресурси. Именно този начин на протичане на процеса на взаимодействие между факторите, определящи развитието на световната мрежа, ще бъде обект на по-подробно разглеждане впоследствие.

От възникването на тези първи три вида онлайн реклама до наши дни са се появили множество техни разновидности, които обаче носят основните характеристики на своите първообрази. Така например, класифицираната реклама се отнася към най-новите видове онлайн реклама, но всъщност има за свой първообраз т.нар. малки обяви или класифицирани рекламни съобщения в пресата. Този вид реклама е изключително проста по отношение на техническата реализация, което я прави евтина и достъпна за по-широк кръг рекламодатели. Предпоставките за реализиране на класифицираната онлайн реклама съществуват много отдавна и може да се смята, че тя е закъсняла с появата си и развитието си в средата на световната мрежа. Можем дори да твърдим, че в този случай маркетинговата мисъл е пропуснала

да се възползва от факторите техническо развитие и физическо разпространение, които отдавна са били на лице.

Още един пример за непълно взаимодействие между трите фактора за развитие на онлайн рекламата са неуспешните и досега опити за създаване на работеща избутана реклама в интернет. При този вид онлайн реклама факторът физическо разпространение е бил налице, но маркетинговата мисъл и техническият напредък до ден днешен не са позволили успешната му реализация.

Възможностите на всеки от трите най-популярни и утвърдени видове онлайн реклама (реклама в електронната поща, банерна реклама и брендинг/спонсорство на уеб страница) са се обогатили с възприемането на интерактивност, директни препратки, анимация, звук. По този начин те продължават да следват схемата на взаимодействие между факторите с цел по-пълно да използват мрежата като канал за комуникация и да я направят по-атрактивна и популярна за всички, които търсят и предлагат. Главоломното развитие на интернет, което продължава и в момента, оправдава това разнообразие на формите и средствата, но както множество изследвания от последно време показват, спада на приходите и резултатите от рекламната дейност в интернет беше съдбоносен за голям брой от т.нар. нови технологични компании (dot.com's), а оцелелите преживяха сериозни сътресения, но за сметка на това откриха нови бизнес модели, които позволиха онлайн рекламата да заеме водещо място в съвременни условия.

Разглеждането на историята на интернет и онлайн рекламата дава добра основа за идентификация на проблемите и по-точното предвиждане на бъдещите пътища за развитие на този маркетингов комуникационен канал. Трите фактора: технически напредък, маркетингова мисъл и физическо разпространение на мрежата са били определящи в миналото и ще продължат да играят тази роля и в бъдеще. Те могат да бъдат полезни и при проследяване на хронологията и движението на цялостната конюнктурата на онлайн бизнеса, част от който е и онлайн рекламата.

От казаното дотук е видно, че интернет и онлайн маркетингът изминаха дълъг път само за последните няколко години. И макар в началото да бе смятана за ограничена, днес практиката показва, че предимствата на мрежата са огромни, като наред с останалите й специфики – глобалност и относителност на времето и местоположението, те обуславят интереса, възможностите, ефективността, трудностите, проблемите, както и предпоставките за бъдещото развитие на онлайн рекламата.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. Clarke, I., Theresa B. Flaherty, Advances in Electronic Marketing, Idea Group Publishing, London 2005.
2. Rogge H. J., Werbung, 6. Auflage, Friedrich Kiehl Verlag, 2004.
3. Огилви Д., Изповедите на един рекламист, Princeps Verlag, Sofia, 1999.
4. Сюзън Тайлър Истман, Дъглас А. Фъргюсън, Робърт А. Клайн, Маркетинг и реклама за електронни медии, кабелни системи и интернет, Слънце Verlag, Sofia 2005.
5. Томс Ж., Интернет рекламата, мисията – възможна. Сиела, С., 2005.
6. Томс Ж., Г. Белушева, Онлайн маркетинг. Мисията още по-възможна, Сиела, С., 2007.
7. Томс Ж., Д. Георгиев, Успешен онлайн маркетинг с 65 примера от практиката, Сиела, С., 2010.

ЕВОЛЮЦИЯ НА НАЧИНИТЕ ЗА ПЛАЩАНЕ НА ОНЛАЙН РЕКЛАМАТА

Светослав Р. Велков
УНИБИТ

Адрес за кореспонденция: 1463 София, ул. „Тунджа" 23, ап. 5

EVOLUTION OF THE METHODS OF PAYMENT FOR ONLINE ADVERTISING

Svetoslav R. Velkov

***ABSTRACT**: Evolution of the payment methods of online advertising is presented as an important aspect for the development and enforcement of advertising on the Internet. Finding a balance in this regard is a continuous process associated with the development of the network and depending on the factors of technical progress, marketing thought and physical distribution of the Internet.*

***KEY WORDS**: Internet, online advertising, payment of online advertising*

От първите си стъпки, направени от т.нар. рекламни банери, които бяха създадени в края на 1994 г. онлайн (on-line) рекламата измина дълъг път и днес тя е неразделна част от живота.

Реклама е всяка платена форма за популяризиране на организация, продукт, услуга или идея, която първоначално е утвърдена в печатните медии, като вестници и списания, а след това в радиото и телевизията. Появата на Интернет измести тези традиционни рекламни канали и през последното десетилетие фокусът се насочи към рекламата във виртуалната среда. По този повод рекламата премина през най-динамичния период в своята история. Технологичният напредък рефлектира в неимоверното нарастване в използването на Интернет, в резултат на което интернет рекламирането се разраства и развива с изключително бързи темпове. Като рекламна среда, Интернет предоставя изключително големи възможности, тъй като могат да се използват различни рекламни формати, за да се предаде рекламното послание, а възможностите за създаване на новаторски, оригинални и грабващи вниманието реклами са практически неизчерпаеми. Все повече големи и малки компании, които до скоро са рекламирали в традиционните медии, прехвърлят голяма част от рекламния си бюджет към on-line рекламата. Последните изследвания в областта на рекламата сочат, че през следващите години онлайн рекламата ще се развива три пъти по-бързо от рекламата в традиционните медии.

Това се дължи на безспорните предимства на интернет рекламата - лесно управление, резултатност, много добри възможности за таргетиране на рекламните съобщения, бързо увеличаваща се аудитория и точно измерване на резултатите, което не може да се постигне при рекламата в традиционните медии. Освен това интернет рекламата комбинира предимствата на телевизионната и печатната рек-

лама и дори предоставя възможността за изключително високо качество на графичното изображение. За разлика от телевизионната, радио и печатна реклама, онлайн рекламите предоставят на потребителите много по-големи възможности за запознаване с продукта или услугата, която се предлага. Рекламният банер може да представя само рекламното съобщение, но всеки заинтересован потребител може без никакви усилия да кликне върху него и да бъде прехвърлен директно към уеб сайта, където подробно да се запознае с предлаганите продукти и услуги, с техните цени и дори да направи поръчка, ако уеб сайта предлага тази възможност. Друго голямо предимство на онлайн рекламата е, че рекламодателят е наясно какво точно получава срещу парите си. Ако той плати 1000 рекламни импресии (показвания на рекламното съобщение) например, той със сигурност знае, че 1000 Интернет потребители ще видят тази реклама.

Разнообразието на Интернет реклама е голямо. Все още изключително популярен остава уеб банерът, който е най-старата форма на Интернет реклама[1]. Текстовият линк е друга форма на on-line реклама, която представлява най-често рекламно мото или име на организация, съдържащо хипервръзка към уеб страницата на рекламодателя. Това е една от най-достъпните и евтини форми на on-line реклама, която същевременно е изключително ефективна. E-mail footer представлява рекламно съобщение, което се добавя в края на всеки изпратен e-mail. Предлага се най-често от уеб сайтовете, които предоставят безплатни електронни пощенски кутии. Платена статия или публикация е друга форма на онлайн рекламата, която се предлага от някои уеб сайтове. Рекламното каре представлява малко рекламно пространство, разположено най-често в някой уеб портал, в което рекламодателят може да публикува своя обява, придружена с малка снимка на своя продукт или фирмено лого. Платената реклама в Google безспорно е една от най-ефективните онлайн реклами, поради масовото използване на тази търсачка от огромен брой Интернет потребители. Анимираната реклама, обхващаща цяла страница е най-скъпият вариант за on-line реклама. Пакетната реклама включва няколко вида от горепосочените форми на on-line реклама. Обикновено рекламодателят сам преценява какви реклами ще включи. При този тип услуга обикновено се правят отстъпки в цената.

Съществува една проста истина и тя е, че рекламодателите трябва да отидат там, където са потенциалните клиенти, за да имат резултат техните рекламни кампании и за да реализират печалби. Все повече от потенциалните клиенти вече са on-line. Интернет е новата среда, в която бизнесът се развива и усъвършенства, а с него и възможностите за реклама и популяризиране на всяка една дейност по новаторски, оригинален и съобразен с аудиторията начин.

Важен аспект при проследяване на историческото развитие на рекламата в интернет е и променящият се с времето начин на нейното таксуване. Заплащането за реклама винаги е бил болезнен въпрос както за рекламодателите, така и за рекламните агенции. Първите поемат риска да платят повече отколкото е оправдано, а вторите съответно да получат по-малко отколкото е заслужено. Намирането на баланс в това отношение е продължителен процес, свързан с развитието на мрежата и също така зависещ от факторите на техническия прогрес, маркетинговата мисъл и физическото разпространение на интернет.

Начините на определяне на заплащането за рекламите в Интернет са няколко. Макар и рядко да се използва, основно за по-малките или специализирани медии,

[1] Първите рекламни банери са пуснати в Интернет в края на 1994 г.

се посочва твърда цена за определено време - година, месец, седмица и т.н. Разпространено е изключително много заплащането на 1000 импресии. Като за PPC (Pay per click) плащането се извършва на клик. Друг начин за определяне на заплащането при Интернет реклама е на действие**.** Това действие може да е някаква покупка, регистрация и т.н. Възможно е заплащане на реален потребител или цена на продажба**.**

Най-динамичното развитие в това отношение може да бъде проследено при банерната реклама. Първият исторически възникнал начин за заплащане на банерната реклама се нарича Flat Fee Advertising и представлява твърда цена за реклама за определен период от време. Този модел на заплащане се е запазил и до днес, но се прилага от по-малките и специализирани медии, които имат тясна аудитория и позволяват специфично таргетиране. Този начин на заплащане е най-опростеният, но в същото време и най-рискованият за двете страни в рекламната сделка.

Тъй като интернет е медия от ново поколение, предлагаща много по-големи и ненадминати досега възможности за обратна връзка с целевата аудитория, той естествено се нуждае и от по-съвършени форми за отчитане на рекламната ефективност. Трите фактора, оказващи влияние върху развитието на интернет играят важна роля и при развитието на начините определяне на цената на рекламата и начините на заплащането й. В този случай маркетинговата мисъл е движещият фактор, който диктува създаването на няколко модерни начина за ценообразуване при онлайн рекламата, първият от които се нарича Cost Per Mille (CPM) или т.нар. цена за 1000 импресии или показвания.

Този модел е подходящ и се прилага при т.нар. интернет портали[2], които събират многобройна и разнообразна аудитория. Това е вторият по ред на възникване вид за заплащане на онлайн рекламата и се прилага за първи път през 1995 година. За съжаление обаче, този механизъм има заложени недостатъци при измерване на реалната честота на показване на рекламата, защото статистическата система може да отчете зареждането на банера от браузъра на потребителя, но по никакъв начин не може да бъде отчетено дали банерът реално е бил показан на екрана на персоналния компютър. Такава ситуация може да възникне когато, например, банерът се намира в долната част на уеб страницата, а потребителят я е напуснал преди да я прегледа изцяло. Или пък банерът се намира в горната част на страницата, но се зарежда със закъснение, когато потребителят вече е насочил вниманието си към друга страница. Съществува и обратната възможност, когато потребителят вижда дадена банерна реклама повече пъти отколкото системата е отчела. Това може да се получи при кеширане[3] на банера, което предотвратява повторното му зареждане, а без зареждане системата не отчита и показване.

За по-пълноценно използване на техническите и статистическите възможности на световната мрежа е разработен моделът за заплащане на онлайн рекламата, наречен Cost Per Click (CPC) или т.нар. цена за натискане върху банерната реклама с посочващото устройство на персоналния компютър. CPC се използва и при заплащането на един нов вид реклама, наречен Ad Words, за който ще стане дума в следващата глава на това изложение. Идеята, която стои зад този модел се състои в това, че техническите възможности на изчислителните машини са в състояние да

[2] Интернет сайтове, които служат като пътеводител или като вход към група специализирани сайтове.

[3] Записване на използвана информация в паметта на уеб браузъра.

засекат и регистрират всяка една проява на интерес от страна на потребителите, което на свой ред не само внася много по-голяма яснота и сигурност в отношенията медия - рекламодател, но също така е и неоценим инструмент в ръцете на специалистите по маркетинг, защото показва много по-точно колко ефективна е дадена рекламна кампания, провеждана онлайн. Този модел макар и по-съвършен от своите предшественици все още не може да отстрани всички неизвестни по пътя от рекламата до продажбата. Много често натискането върху рекламния банер от страна на потребителя е инцидентно или крие зад себе си съвсем различни подбуди от желанието за получаване на информация за даден продукт или услуга, или пък за извършването на покупка.

Следващият по хронологичен ред и също така по-точен начин за отчитане на работата на онлайн рекламата се нарича Cost Per Action (CPA). При него ефективността на рекламното послание се свърза директно с постигната продажба или друг резултат. Неговото разпространение обаче е все още ограничено и се прилага основно при електронни магазини (където има възможност за електронна продажба) или при продукти и услуги от интелектуален характер (софтуер, сайтове с платено съдържание и др.), чието консумиране е възможно директно чрез интернет.

Ценовият модел CPS (Cost Per Sale), както и CPA свързва директно степента на въздействие на рекламата с продажбата на рекламираната стока или услуга. За разлика от CPA, CPS се определя като процент от стойността на извършената продажба, което дава много ясна представа за приноса на рекламата в извършването на една единствена продажба.

Когато сравним изброените до тук ценови модели можем да направим следните заключения:

- първият ценови модел (Flat Fee Advertising) е най-изгоден за рекламната агенция, защото заплащането не се влияе от реалната работа на рекламата, т.е. издателят получава парите си независимо от всичко;

- при модела CPM заплащането зависи до голяма степен от посещаемостта на уеб сайта (на рекламиращата медия), но не зависи от качеството на самото рекламно послание; при третият вариант (CPC) на заплащане под внимание се взима както посещаемостта на уеб страницата, така и качеството на рекламното послание (само по себе си, тъй като качеството на рекламата се оценява по това колко продажби извършва);

- последните два модела (CPA и CPS) отчитат всички фактори за наистина успешната работа на рекламата и се прилагат успешно само в интернет (другите нямат необходимите възможности за да използват тези ценови модели).

Изложеното дотук не означава, че рекламните агенции се стремят единствено към сделки включващи първия ценови модел (Flat Fee Advertising), а рекламодателите към такива включващи само последните два модела (CPA и CPS), защото тези съотношения са регулирани от сравнителните пропорции между цените за всеки от моделите, т.е. гарантираната за заплащане реклама е несравнимо по-евтина от реално работещата реклама (разликата достига до над 1000 пъти). Ето защо интересите на двете страни – рекламодател и рекламна агенция обикновено се срещат някъде по средата, което е и обяснението за това, че моделите CPM и CPC са най-разпространените в наше време.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. Clarke, I., Theresa B. Flaherty, Advances in Electronic Marketing, Idea Group Publishing, London 2005.
2. Rogge H. J., Werbung, 6. Auflage, Friedrich Kiehl Verlag, 2004.
3. Огилви Д., Изповедите на един рекламист, Princeps Verlag, Sofia, 1999.
4. Сюзън Тайлър Истман, Дъглас А. Фъргюсън, Робърт А. Клайн, Маркетинг и реклама за електронни медии, кабелни системи и интернет, Слънце Verlag, Sofia 2005.
5. Томс Ж., Интернет рекламата, мисията – възможна. Сиела, С., 2005.
6. Томс Ж., Г. Белушева, Онлайн маркетинг. Мисията още по-възможна, Сиела, С., 2007.
7. Томс Ж., Д. Георгиев, Успешен онлайн маркетинг с 65 примера от практиката, Сиела, С., 2010.

ВЪЗМОЖНОСТИ ЗА ПРИЛАГАНЕ НА НОВИ ТЕХНОЛОГИИ И МАРКЕТИНГОВИ КОНЦЕПЦИИ В ОНЛАЙН РЕКЛАМАТА

Светослав Р. Велков
УНИБИТ

Адрес за кореспонденция: 1463 София, ул. „Тунджа" 23, ап. 5

OPPORTUNITIES APPLICATION OF NEW TECHNOLOGIES AND THE MARKETING CONCEPT IN ONLINE ADVERTISING

Svetoslav R. Velkov

ABSTRACT: *Presents opportunities for the application of new technologies and marketing concepts as a prerequisite for the development of online advertising.*

***KEY WORDS**: Internet, online advertising, marketing, Technology for the control of data flows, Permission-Push-Pay-off advertisement*

Онлайн рекламата е относително млада и нейната роля в маркетинговия комуникационен микс на фирмата все още не е достатъчно добре определена. Съвременният пазар с жестоката си конкуренция налага постоянно и систематично въздействие върху потребителите, които както е казал Робърт Рийвс: "трудно запомнят, затова пък са склонни да забравят"[1]. Маркетинговите специалисти се сблъскват с проблема, че трябва да създават кратки и убедителни рекламни послания в условията на една изобилстваща от информация медия и да се опитат да направят тези рекламни послания достояние на колкото се може по-голям брой потребители, при положение, че не могат (и не бива) да използват похватите на натрапващия маркетинг.

[1] Огилви Д., Изповедите на един рекламист, Princeps Verlag, Sofia, 1999с. 163.

Идеята за прилагане на избутващата технология (push) в условията на световната мрежа не е нова. Може да се каже, че форми на избутване на реклама и информация в мрежата се прилагат много отдавна. Това се осъществява с помощта на т.нар. Cookies (бисквити), които представляват малки програми, заложени в уеб страниците, които позволяват на даден интернет сайт да проследява своите потребители. По този начин „провайдърите на интернет услуги, търсачките и уеб сайтовете по оригинален начин доставят информация на потребителите си („бутат" я автоматично), без те да са молили за това"[2]. Злоупотребата с информацията намираща се в „бисквитите", която се използва за събиране на електронни адреси на потребителите с цел директна реклама, скоро компрометира и този маркетингов механизъм. Стига се да момент, в който много непочтени интернет страници търгуват с потребителската информация, в резултат на което потребителите биват заливани с нежелани поп-ъпи и електронна поща. В наши дни всички уеб браузъри имат способността да блокират програмите, наречени „бисквитки" и тази способност е активирана по подразбиране.

Компанията Point Cast, която е основана през 1992 г. е може би първата, която започва да прилага явна „избутваща" технология в интернет. Нейният продукт представлява софтуерен клиент – програма, която се зарежда на компютрите на потребителите и осъществява връзка с излъчващия сървър. По този начин канализирана информация достига до потребителите без да е необходимо тяхното участие. Използват се промеждутъците, в които се включва screensaver на компютъра, но вместо него на екрана започва да се излъчва канализираната информация. Услугата и софтуерният клиент са били безплатни за потребителите като компанията се е финансирала от реклама, която е била излъчвана по посочения начин.

Point Cast е пионер в използването на избутващата технология, която ще бъде изключително важна за интернет в бъдеще. За съжаление обаче Point Cast става жертва първо на това, че значително изпреварва времето си и второ на това, че компанията, по мнението на анализаторите, е била управлявана недостатъчно добре. Лошата съдба на компанията Point Cast насочва другите две по значими IT компании – Back Web и Marimba, които развиват и използват избутващи технологии към пазарни сегменти, които нямат нищо общо с излъчването на канализирана информация в интернет.

Това, което отличава интернет каналите от традиционните избутващи медии е, че излъчваната информация може да бъде персонализирана от самите потребители. Това е и основното предимство, което евентуално са имали фирмите като Point Cast, и което имат днес съвременните фирми прилагащи форми на избутващата технология в интернет. Предлаганите от тези фирми услуги са безплатни за потребителите, но от друга страна потребителите все пак са заплащали за тях с натрупаният допълнителен трафик.

Докато получаването на канализирана информация от рода на специализирани новини от дадена област продължава да работи и до наши дни под формата на най-различни "newsletters", то изпращането на канализирана реклама не успява да се върне на пазара. За обяснението на неуспеха на ранните форми на избутаната рек-

[2] Сюзън Тайлър Истман, Дъглас А. Фъргюсън и Робърт А. Клайн, Маркетинг и реклама за електронни медии, Изд. Слънце, С., 2005, с. 385.

лама в интернет могат да бъдат взети под внимание някои от факторите, които оказват негативно влияние и върху „традиционната" онлайн реклама.

Така както и останалите форми на онлайн реклама, избутаната (канализирана) реклама трябва да се бори с пренасищането на мрежата с рекламни послания. Затова не може да се очаква, че потребителите биха предпочели канализираната реклама само и единствено защото тя се селектира в съответствие с техните интереси.

Друг недостатък, който също е общ за ранните форми на избутаната реклама и за останалата онлайн реклама, е този, че всички те струват на потребителите време и пари, тъй като генерират трафик и забавят скоростта на достъп. Избутаната реклама използвана в интернет преди е служела за да финансира услугата по доставка на подбрана информация и новини до клиентите, което отново бива заплащано от потребителите.

От казаното дотук става ясно, че и ранните форми на избутаната онлайн реклама притежават сериозни недостатъци, и подобно на останалите видове онлайн реклама нямат реални шансове за постигане на добри, работещи резултати. Това обаче не означава, че канализирането на рекламните послания и тяхното избутване през мрежата е загубена кауза. Тук по-скоро става въпрос на проява на т.нар. „детски болести" на една концепция, която има добър потенциал.

Развитието на световната мрежа, което се подчинява на факторите, които бяха описани в първа глава на тази работа (технологично развитие, маркетингова мисъл и физическо разпространение), продължават да са в сила и днес. На бял свят се появяват нови технологии, които предоставят нови възможности. Две от тези нови технологии дават шансове на концепцията за избутана, канализирана и индивидуализирана онлайн реклама да намери ново приложение, да заработи в полза на потребителите и да генерира реални бизнес резултати.

Технология за контрол на потоците от данни

За разлика от съществуващите досега технологии за избутване на информацията към потребителя, тази технология има предимството, че не изисква инсталация на какъвто и да било софтуер на компютъра на клиента.

Друго основно предимство на технологията е, че тя не зависи от интернет браузъра на индивидуалния потребител. Това означава, че има осъществяване на реално излъчване на информацията, което не може да бъде пропуснато или заобиколено. Излъчваната информация се контролира изцяло от доставчика на Интернет и не се конкурира с никакви други потоци от данни.

Устройства, които използват новата технология вече са на пазара и някои от големите телекомуникационни компании в Европа (като Deutsche Telekom AG) вече експериментират в областта на управлението на потоците от данни.

Технологии за гарантиране на качеството на услугата (Quality of Service).

Quality of Service (или съкратено QoS) е понятие, което навлиза все по-бързо на пазара на телекомуникационните услуги. През следващите няколко години ще станем свидетели на неговото въвеждане и в областта на доставка на интернет.

Така например световно известната компания Cisco Systems, която е лидер на пазара за мрежово базирани решения определя QoS като: „възможността на определена мрежа да осигурява по-добро обслужване на избран трафик от данни".

Технологиите за осигуряване на QoS ще играят важна роля за оформянето на пазара за доставка на интернет и също така предоставят възможност за интегрирането на избутаната онлайн реклама.

Резултатът от контрола върху качеството на доставката на интернет до потребителя може да се обобщи в следното: потребителите ще имат възможност да избират на какво ниво да бъдат обслужвани, като съответно за всяко по-високо от стандартното ниво на обслужване те ще трябва да заплащат по-скъпо.

При интегриране на избутаната онлайн реклама в системата за контрол на качеството на обслужване потребителите сами ще имат възможността да определят колко и каква избутана реклама да получават и дали въобще желаят да получават реклама. В тази си дейност потребителите ще се ръководят от факта, че получаването на реклама ще работи в тяхна полза. Иначе казано избутаната онлайн реклама ще бъде ефективен инструмент за регулиране на разходите за ползването на интернет. Това ще бъде така, защото получаването на онлайн реклама, за първи път в историята на интернет, няма да носи разходи, а напротив реално осезаеми приходи за потребителите.

Концепция за закупуване на вниманието на потребителите.

Поради факта, че много от очакванията по отношение на онлайн рекламата не са оправдани, маркетинговите специалисти започват да търсят начини за повишаване на ефективността на рекламата в световната мрежа. Най-съществения проблем в това отношение продължава да бъде този дали рекламата достига до своите истински адресати. В опит да бъде решен генерално този проблем се появява и концепцията за закупуване на потребителското внимание.

През 1995 г. Нат Голдхабър възприема идеите на своя братовчед философ за това, че съвременното общество все повече се превръща в „общество на вниманието", където най-високата ценност, която някой може да плати е неговото внимание и основава компанията CyberGold. CyberGold съчетава концепцията за вниманието като скъпо струваща стока с интерактивността, мултимедийния характер и проследяващите възможности на световната мрежа.

Концепцията на работа на CyberGold се състои в това, че се очаква, че рекламодателите ще бъдат готови да заплатят известна цена на потенциалните клиенти в замяна на тяхното внимание по отношение на информация за предлаган продукт. Концепцията първоначално изглежда странна, имайки предвид съвременното разбиране сред по-голямата част от хората, че рекламата е нежелан, излъчван в ефира шум. CyberGold обаче се опитва да промени из основи установените правила на „рекламната игра" и започва да предлага място във виртуалното пространство, където да се срещнат заинтересувани рекламодатели и потребители.

След като веднъж са намери рекламодатели и заинтересувани потенциални купувачи, тези заинтересувани потенциални купувачи се съгласяват да получават реклама, която до голяма степен отговаря на насоките на тяхното търсене и вече не се смята за нежелана. За да бъде намерена реклама отговаряща на техните интереси, потребителите трябва да попълнят въпросници.

При всяко посещение на уеб страницата на CyberGold, компанията събира все повече данни за абонатите. Записва се информация като време прекарано върху конкретна реклама, кои точно реклами са избрани и в каква последователност, къде точно потребителите избират да кликнат върху рекламата, по кое време на деня потребителите влизат в системата и дали отговарят на въпросите свързани с получаваната реклама и дали го правят добросъвестно. CyberGold съчетава тази информация с информацията от други полеви проучвания и въпросници и продължава да води записки през цялото време на отношенията си със своите абонати.

CyberGold разширява обхвата на концепцията си като не само заплаща на своите абонати за това, че получават реклама, която реално ги интересува, но и се възползва от интерактивността и мултимедийния характер на интернет. Компанията се опитва да направи процеса на събиране на данни и гледането на реклама от потребителите по развлекателен и предлага на абонатите си прости онлайн игри, допълнителна информация и квизове.

Компанията заплаща вниманието само на онези абонати, които участват активно в рекламния процес. Потребителите трябва да предприемат някакво конкретно действие или да преминат квиз, който е част от рекламата за да им бъде заплатено тяхното внимание. По този начин CyberGold гарантира на рекламодателите, че потенциалните клиенти са въвлечени в рекламния процес.

Заплащането на купеното внимание се осъществява в т.нар „CyberGold", което се изразява в пари в брой, ваучери за пътуване със самолет или благотворителни подаръци. Компанията има намерение да промени начина на заплащане и да премине изцяло към електронно разплащане със своите абонати. Проблемът с безпрепятственото разплащане с потребителите е важен, защото той е определящ за това колко клиенти може да привлече и да обслужва компанията.

Концепцията на CyberGold е нова и предлага радикален подход за промяна на рекламния бизнес в интернет. За да може да се сдобие с успех обаче трябва да бъдат преодолени проблеми, свързани с установените схващания за рекламата, технологични, културни и бизнес бариери.

През 2000 година CyberGold е закупена за 157 млн. долара от компанията MyPoint Inc., с което се създава и най-голямата компания за лоялен маркетинг в сферата на интернет. Новосъздадената компания Nectentives Inc. става лидер на пазара за закупуване на потребителското внимание, но само година по-късно тя обявява банкрут.

Неуспехът на Nectentives Inc. се дължи основно на рязкото свиване на онлайн бизнеса и забавянето в неговото развитие. Както и много други, компанията става жертва на динамичния характер на онлайн средата в онези години, които подтикват мениджърите да инвестират големи суми, които се оказват безвъзвратно изгубени след колапса на пазара през 2000 г.

Концепцията за закупеното потребителско внимание днес е част от инструментариума на лоялния маркетинг, чиято цел е да създава, изгражда и задълбочава връзките с клиентите на фирмата.

Permission-Push-Pay-off реклама

Наблюдавайки тенденциите в развитието на телекомуникационните технологии и използвайки исторически утвърдените начини за протичане на процеса на адаптация на новите технологии в интернет и онлайн рекламата, може да се предположи, че е настъпил моментът, в който технологията за избутване на данни през мрежата да бъде използвана за създаването на онлайн реклама от нов вид.

Реалното излъчване на данни, съчетано с възможностите за контрол на качеството на услугата (предоставяне на достъп до интернет) дава по-големи шансове за успех на този модел, отколкото успеха на неговите предшественици.

От друга страна, моделът трябва да бъде съобразен така, че да съчетава предимствата и да изключва недостатъците на традиционните форми на онлайн рекламата, които бяха разгледани във втора глава на тази работа.

Вземайки горепосочените изводи и заключения за водещи, ние можем да предложим Permission-Push-Pay-off модела за онлайн реклама, чиято същност и начин на работа ще бъдат разгледани по-долу.

Начинът на работа на онлайн рекламата, която използва най-новите технологии за избутване на данни в Интернет и системата за контрол на качеството на обслужване може да бъде наречен Permission-Push-Pay-off. Това е така, защото системата за контрол на качеството на услугата изрично изисква съгласието на потребителя за това дали той иска да получава реклама (Permission); защото системите за избутване и контрол на потоците от данни в интернет гарантират изпълнението на сключения между потребителя и доставчика на интернет договор, тъй като не зависят от намесата на потребителя и не могат да бъдат заобиколени (Push); защото рекламата, която получава потребителят е наистина безплатна за него и дори му носи предимства (Pay-off).

В случая, източникът на избутаната реклама е доставчикът на интернет. Това означава, че рекламните агенции и директните рекламодатели ще трябва да се свързват директно или чрез посредник с доставчика на интернет, за да могат да публикуват рекламни послания. Тази организация на рекламното разпространение естествено дава предимство на по-големите доставчици на интернет, които имат повече клиенти, а с това и по-голяма целева аудитория, която може да бъде таргетирана от рекламните агенции.

Избутаната реклама от този тип може да бъде организирана на принципа на класифицираната реклама в интернет. В този случай потребителите ще имат възможност периодично да заявяват своите интереси и да получават релевантна на тях реклама. Така ще бъде избегнат проблема с получаването на рекламни послания от потребители, които не се интересуват от тях и ще се повиши процента на достигане до целевата аудитория. Т. е. в много голяма степен ще бъде избегнато негативното отношение на потребителите към реклама, която не ги интересува и само отнема тяхното време. По този начин значително ще бъде ограничен рискът от това, че „опитвайки се чрез рекламата да достигнем едновременно до всички, всъщност не достигаме до никого”[3].

Дори и при начините за плащане онлайн рекламата от този нов вид може да бъде изключително гъвкава. Това е така, защото интерактивността на интернет и съвременните системи за измерване на показателите като времетраене и реакция на потребителите на рекламното послание позволяват едновременното прилагане на няколко различни модела за плащане на избутаната реклама от типа Permission-Push-Pay-off. Така например излъчването на рекламните послания може да се осъществява последователно за определени периоди от време по модела на телевизионните рекламни спотове и да бъде заплащано по същия начин. Тъй като обаче спотовете ще бъдат интерактивни, т.е. докато тече спотът потребителите ще имат възможността да бъдат отведени да интернет сайта на рекламодателя, за да получат допълнителна информация или за да извършат директна покупка. В този случай освен заплащането за времето за излъчване на рекламния спот, на рекламодателите ще бъдат начислени и разходи по модела CPC (Cost Per Click) и CPA (Cost Per Action). Тези допълнителни разходи са оправдани за рекламодателя, защото позво-

[3] Сюзън Тайлър Истман, Дъглас А. Фъргюсън и Робърт А. Клайн, Маркетинг и реклама за електронни медии, Изд. Слънце, С., 2005, с. 24.

ляват на неговата реклама да генерира реален бизнес и за потребителя, тъй като го стимулират с по-висока възвръщаемост от получаването на онлайн реклама.

Рекламата от предложения вариант е гъвкава и по отношения на т.нар креатив. Това означава, че при оформянето на рекламното послание рекламните специалисти няма да бъдат ограничавани от факторите като място, обем на излъчените данни, качество на картината, наличие на звук и анимация. Това е така защото излъчената реклама, чийто източник и доставчикът на интернет няма да се конкурира с никакви други потоци от данни и ще има на свое разположение площта на целия на монитор на потребителя. Рекламното послание няма да бъде вмъкнато между друга информация както това става на уеб сайтовете.

Другият положителен аспект при оформянето на рекламата по този начин е че ще бъде избегнато генерирането на скъпо струващ за потребителите трафик. Основния фактор, които оказва влияние върху цената и качеството на доставката на интернет е т.нар. пиъринг. Пиърингът е понятие, което се използва за обозначаване на входящия и изходящия трафик от дадена самостоятелна мрежа, която е част от интернет, към други самостоятелни мрежи. В световната практика пиъринг отношенията се регулират на реципрочна основа. Това означава че всеки две, свързани една с друга мрежи регулират отношенията си билатерално. Когато потребителите на една мрежа предизвикат трафик в съответната партньорска мрежа, този трафик трябва да бъде заплатен при положение, че надхвърля предизвикания от потребителите на партньорската мрежа трафик в мрежата домакин. Опростено казано, колкото една мрежа е по-малка, толкова по-скъпа става доставката на интернет за нейните потребители, защото те ще бъдат принудени да търсят повече ресурси извън мрежата домакин, а потребителите на по-големите партньорски мрежи няма да предизвикват компенсиращ реципрочен трафик. По този модел малките доставчици не могат да си позволят да предоставят високо качество на услугата, тъй като всеки изходящ от тяхната мрежа трафик им струва скъпо. С прехвърлянето на рекламата на нивото на доставчика на интернет, трафикът на данни предизвикан по този начин остава вътрешно мрежов и съответно много по-евтин.

Предложеният вид избутана онлайн реклама се характеризира с това, че е организиран на местно ниво. Това както вече споменахме може да въздейства благоприятно върху отварянето на рекламния пазар за малки и средни рекламодатели, които са приемали мрежата като неефективен комуникационен канал. Локализирането на рекламата ще повиши нейната релевантност и е възможно да я направи привлекателна за много по-голям брой браншове. Ако онлайн рекламата бъде организирана по този начин тя може да измени положението на интернет, като го превърне от допълващ маркетингов канал, който се използва от по-големите рекламодатели за цялостно покриване на пазара в рекламна медия с реални конкурентни предимства пред радиото и телевизията.

Глобалния характер на мрежата, който до този момент облагодетелства основно мултинационалните компании също ще запази своите преимущества и дори може да бъде благоприятно повлиян от адаптирането на рекламните послания за местната аудитория. Тази адаптация ще се състои основно в превеждане на рекламата на местния език и фина настройка на посланията според местната култура и разбирания.

Освен всички предимства, които интерактивното пространство на интернет предоставя на рекламата като мултимедия (възможност за комуникация с помощта

на текст, картина, звук и интерактивност), Permission-Push-Pay-off рекламата съдържа в себе си и следните предимства:

- коректност по отношение на потребителите, които от една страна имат възможност да изберат дали да получават реклама, а от друга могат да изпитат благоприятен ефект от получаването на рекламата;
- ефективно адресиране на целевата аудитория според нейните езикови и културни особености;
- потребителите имат възможността да определят тематиката на рекламата, което повишава степента на достигане до целевата аудитория;
- потребителските интереси и системата за печелене от получаването на реклама могат да бъдат обхванати ефективно на локално и регионално ниво;
- ефективно отваряне на рекламния пазар в интернет за местните малки и средни рекламодатели, тъй като организирането на рекламните кампании може да се мащабизира (град, регион, държава и т.н.) в зависимост от обхвата на доставчиците на интернет и рекламните агенции;
- гъвкаво заплащане на рекламата, което стимулира потребителите и е изгодно за рекламодателите.

Недостатъци на Permission-Push-Pay-off рекламата:

- бавно навлизане на новите технологии за контрол на потоците от данни и управление на качеството на услугата, които първоначално ще бъдат изключително скъпи за по-малките доставчици на интернет;
- пречки от легислативен характер, отнасящи се до контрола на данните на индивидуалния потребител, с който доставчиците на интернет се сблъскват още днес;
- предложеният вариант на онлайн реклама е подходящ в много по-голяма степен за домашните потребители на интернет, тъй като е много вероятно бизнес потребителите да предпочетат бърз и безпрепятствен достъп до интернет (по-високо качество на услугата), макар и с по-висока цена;
- ниско равнище на цените за достъп до интернет, което намалява значително атрактивността на Pay-off функцията на предложения рекламен вариант;
- несъвместимост на предложения модел със status quo в рекламния бизнес в интернет в наши дни.

Макар и сериозни, посочените недостатъци на предложения вид онлайн реклама не са непреодолими. Те адресират основно проблеми на световната мрежа и онлайн рекламата като цяло, които по един или друг начин трябва да бъдат решени.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. Clarke, I., Theresa B. Flaherty, Advances in Electronic Marketing, Idea Group Publishing, London 2005.
2. Rogge H. J., Werbung, 6. Auflage, Friedrich Kiehl Verlag, 2004.
3. Огилви Д., Изповедите на един рекламист, Princeps Verlag, Sofia, 1999.
4. Сюзън Тайлър Истман, Дъглас А. Фъргюсън, Робърт А. Клайн, Маркетинг и реклама за електронни медии, кабелни системи и интернет, Слънце Verlag, Sofia 2005.
5. Томс Ж., Интернет рекламата, мисията – възможна. Сиела, С., 2005.
6. Томс Ж., Г. Белушева, Онлайн маркетинг. Мисията още по-възможна, Сиела, С., 2007.
7. Томс Ж., Д. Георгиев, Успешен онлайн маркетинг с 65 примера от практиката, Сиела, С., 2010.

ПОЛИТИКИ НА РУСКАТА ФЕДЕРАЦИЯ ПРИ УПРАВЛЕНИЕ НА КРИЗИ

Здравко Ю. Кузманов

Шумен ул. „Карел Шкорпил" 1 Факултет „Артилерия, ПВО и КИС"

POLICY OF THE RUSSIAN FEDERATION IN CRISIS MANAGEMENT

Zdravko Y. Kuzmanov

Shumen, 1 Karel Shkorpil Str., Faculty of Artillery, Air Defence and CIS

KEY WORDS: *Russian Federation, Crisis Management, policies.*

Единната национална система за оповестяване и ликвидация при извънредни ситуации (Единая государственная система предупреждения и ликвидации чрезвычайных ситуаций – РСЧС) е предназначена за защита на населението и територията на страната при възникнали извънредни ситуации от природен, техногенен или друг характер, обезпечаване в мирно време на сигурността на населението, територията и обкръжаващата среда, материалните и културни ценности на държавата. [1] Системата обединява органите за управление, силите и средствата на федералните органи на изпълнителната власт, органите на изпълнителната власт в субектите на РФ, органите за местно самоуправление, организации (в т.ч. частни), при изпълнението на политиките и решенията касаещи въпросите по защита на населението и територията при извънредни ситуации. [2]

Основните задачи на РСЧС, включват: [2]

- разработка и реализация на правни и икономически норми за обезпечаване на защитата на населението и територията при извънредни ситуации и обезпечаване на устойчивото функциониране на предприятия, учреждения и организации в такива ситуации;
- осъществяване на целеви и научно-технически програми, по направление ранно оповестяване при извънредни ситуации и обезпечаване на устойчиво функциониране на предприятия, учреждения и организации при такива ситуации;
- обезпечаване на готовността за действие на органите за управление, силите и средствата, предназначени за ранно оповестяване и ликвидация при извънредни ситуации;
- събиране, обработка, обмен и използване на информация в областта на защитата на населението и територията при извънредни ситуации;
- подготовка на населението при извънредни ситуации;
- осъществяване на държавни експертизи, надзор и контрол в областта на защитата на населението и територията при извънредни ситуации;
- ликвидация при извънредни ситуации;

- осъществяване на социални мерки за пострадали при извънредни ситуации, провеждане на хуманитарни операции;
- реализация на правата и задълженията на гражданите в областта на защитата при извънредни ситуации;
- международно сътрудничество в областта на защитата на населението и територията при извънредни ситуации.

Организационната структура на РСЧС се състои от териториални и функционални подсистеми. Има пет нива:
- *федерално ниво,* обхваща цялата територия на РФ;
- *междурегионално ниво,* обхваща територията на няколко субекта на РФ;
- *регионално ниво,* обхваща територията на субект на РФ;
- *общинско ниво,* обхваща територията на общинска единица;
- *обектно ниво,* обхваща територията на производствен или социален обект.

Териториалните подсистеми на РСЧС се създават на територията на субектите на РФ и се състоят от звена, съответстващи на административно-териториалното деление. Функционалните подсистеми на РСЧС се създават във федералните органи на изпълнителната власт.

Органите за управление на РСЧС включват координиращи, за ежедневно управление и постоянно действащи.

Координиращи органи са:
- *на федерално ниво* – Правителствена комисия за предупреждение и ликвидация при извънредни ситуации и обезпечаване на противопожарната безопасност, комисии за предупреждение и ликвидация при извънредни ситуации и обезпечаване на противопожарната безопасност на федералните органи на изпълнителната власт и упълномощени организации, имащи функционални подсистеми на РСЧС;
- *на регионално ниво* (в предела на територията на субекта на РФ) – Комисия за предупреждение и ликвидация при извънредни ситуации и обезпечаване на противопожарната безопасност на органа на изпълнителната власт в субекта;
- *на общинско ниво* (в предела на територията на общинската единица) – Комисия за предупреждение и ликвидация при извънредни ситуации и обезпечаване на противопожарната безопасност на органа за местно самоуправление;
- *на обектно ниво* – Комисия за предупреждение и ликвидация при извънредни ситуации и обезпечаване на противопожарната безопасност.

Органи за ежедневно управление са:
- *на федерално ниво – Национален център за управление при кризи* (Национальный центр управления в кризисных ситуациях – НЦУКС);
- *на междурегионално ниво* – Център за управление при кризисни ситуации, регионални центрове на Министерство на извънредните ситуации (МЧС);
- *на регионално ниво* – Център за управление при кризисни ситуации, Главни управления на МЧС;
- *на общинско ниво* – Единни дежурно-диспечерски служби на общинските единици;
- *на обектно ниво* – дежурно-диспечерски служби на предприятията.

Постоянно действащи органи:

- *на федерално ниво* – Министерство на извънредните ситуации;
- *на междурегионално ниво* – Регионални центрове на МЧС;
- *на регионално ниво* – комисии, Главни управления на МЧС в субектите на РФ;
- *на общинско ниво* – органи, специално упълномощени за решаване на задачи в областта на защитата на населението и територията при извънредни ситуации и/или гражданска защита при органите за местно самоуправление;
- *на обектно ниво* –структурни подразделения на организацията, упълномощени за решаване на задачи в областта на защитата на населението и територията при извънредни ситуации и/или гражданска защита.

НЦУКС е органа за всекидневно управление на националната система РСЧС. Предназначен е за обезпечаване на дейностите на МЧС за управление в областта на гражданската защита, защитата на населението и територията при извънредни ситуации, противопожарна безопасност, безопасност на населението и водните обекти, а също и координация по установения ред на дейностите на органите на изпълнителната власт в рамките на РСЧС. [3]

В числото на задачите на НЦУСК влизат:

- подготовка и предложения за приемане на дежурни сили и средства;
- обезпечаване на оперативното управление на РСЧС в хода на изпълнение на мероприятия по оповестяване и ликвидация при извънредни ситуации;
- контрол върху готовността на подразделенията за оперативно реагиране;
- оповестяване и информиране на населението за прогнозируеми и възникнали извънредни ситуации и пожари.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. Интернет-портал Правительства Российской Федерации. 2013, <http://government.ru>.
2. Федеральный закон от 21 декабря 1994 г. No 68-ФЗ, „О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера“. изм. 2013, <http://base.garant.ru>.
3. МЧС России. Силы и средства : Национальный центр управления в кризисных ситуациях МЧС России. 2013, МЧС, < http://www.mchs.gov.ru>.

ПОЛИТИКИ НА ЕВРОПЕЙСКИЯ СЪЮЗ ПРИ УПРАВЛЕНИЕ НА КРИЗИ

Здравко Ю. Кузманов

Шумен ул. „Карел Шкорпил" 1 Факултет „Артилерия, ПВО и КИС"

EUROPEAN UNION POLICY ON CRISIS MANAGEMENT

Zdravko Y. Kuzmanov

Shumen, 1 Karel Shkorpil Str., Faculty of Artillery, Air Defence and CIS

KEY WORDS: *European Union, Czech Republic, Crisis Management, policies.*

Към настоящия момент европейската система **за управление при кризи** се намира на етап изграждане. Съществуват две направления, първото засяга *Европейската политика за сигурност и отбрана* – ЕПСО (European Security and Defence Policy), а второто *Европеска политика за защита при бедствия и хуманитарна помощ*. [1]

Управлението при кризи на ниво ЕС се осъществява в хода на операции и мисии съгласно ЕПСО, които по своето предназначение, мащаб, решаеми задачи, привлечени сили и средства, съгласно преценката на ръководството на Евросъюза, се подразделят на военни, полицейски, за поддържане на мира („върховенство на закона") и наблюдателни. Операциите по управление на кризи съдържат военен компонент, докато мисиите са с граждански характер.

Военните операции се провеждат с цел разделяне на враждуващите страни и установяване на мир в района на кризата.

Полицейските мисии са предназначени за стабилизиране на обстановката вътре в страната и подпомагане на процесите по формиране и подготовка на дееспособни органи за поддържане на обществени ред, по правило, в след кризисния период.

Мисиите на ЕС за поддържане на мира са насочени към оказване на помощ за правителствата на заинтересованите страни в процеса на реформиране на силовите структури. Установяване на държавната власт и съдебно-правовата система с цел задействане и развитие в държавата на демократични и правови норми.

Наблюдателните мисии се организират от Евросъюза за осъществяване на контрол над изпълнението на постигнатите договорености между противостоящите страни.

В качеството на основни механизми за кризисно регулиране ЕС разглежда военния потенциал и гражданските антикризисни структури.

Към първите се отнасят силите за реагиране на съюза, състоящи се от разнородни въоръжени компоненти, предназначени за провеждане на антикризисни, миротворчески и хуманитарни операции. Те са считани за основно силово средство за защита на интересите на страните от Евросъюза, в това число в отдалечени за територията на Европа региони.

Друг инструмент, приет от ЕС при регулирането на кризисни ситуации и преодоляването на последствията от тях, се явяват специалните граждански антикризисни сили, които чрез невоенни методи съдействат и решават задачи при възстановяване в засегнати територии.

По състав гражданските антикризисни структури представляват военизирани и граждански формирования на страните-членки, включващи: подразделения на полицията, жандармерията, групи специалисти по административно управление, структури на представители на правосъдието, отряди на гражданска защита и международни наблюдатели.

Тези структури са способни самостоятелно или във взаимодействие със силите за реагиране на Евросъюза да обезпечат: поддържане на обществения ред в кризисните райони; решаване на задачи свързани с борбата с престъпността; осъществяване на граничен контрол; съдействие на правораздавателните органи; подготовка на кадри; оказване на хуманитарна помощ на населението; провеждане на спасително-издирвателни и възстановителни операции; изпълнение на функции по линия на международни наблюдатели.

Важно направление в дейността на гражданските антикризисни структури на ЕС се явява оперативното обезпечаване и реагиране при стихийни бедствия, във всяка точка по света, с цел локализация на последствията и недопускане на хуманитарна катастрофа.

Като цяло за ЕС, процеса на управление при кризи е съпътстван от силна институционална фрагментация. Към момента има три институции ангажирани с въпросите по провеждане на политиката за управление при кризи – Съветът ЕС (Съветът по външни работи), Европейска служба за външна дейност и Европейската комисия. [1]

Основен орган към Европейската комисия отговарящ за кризи от тип бедствия е Главна дирекция „Хуманитарна помощ и гражданска защита“. Главните механизми за отговор при кризи по направление гражданска защита на дирекцията е Европейския механизъм за гражданска защита. Механизмът работи чрез Центъра за мониторинг и информация (ЦМИ), управляван от Европейската комисия и активен 24/7. Всяка държава, засегната от голямо бедствие, в ЕС или извън него, може да поиска помощ чрез центъра, който незабавно препраща искането до мрежа от органи за контакт в 32 страни, участващи в Механизма. Центърът координира помощта, предоставена от тях.

За анализирането на европейския опит в управлението при кризи е необходимо да бъде извършен анализ на състоянието и политиките при управление на кризи на конкретно избрани държави-членки на Европейския съюз. Една такава държава – Чешката република е с относително сходна на Р. България по територия и брой на населението страна, също преминаваща през процесите на децентрализация и преход към пазарна икономика в последните повече от две десетилетия.

Системата за **управление при кризи,** в условия на политиката за сигурност на Чешката република се счита за комплекс от процедури и разпоредби, управляващи действията на съответните органи на публичната администрация и на други заинтересовани страни, за преодоляване на неблагоприятното разгръщане на кризи в обществото. Елементите на системата са систематизирани в разпоредбите на Закон № 240/2000 относно управлението на кризи. [2]

Системата за управление при кризи на ЧР се ръководи от националното правителство и включва: Съвет за национална сигурност; Централен кризисен щаб; Разузнавателна работна група, към Информационната служба за сигурност; Координационен център по въпросите на борбата с финансирането на тероризма. [3]

Съветът за национална сигурност е постоянно действащ орган на правителството и отговаря за координирането на въпросите свързани със сигурността на страната и подготовка на проектни мерки за нейното гарантиране. [4] Ръководи се от министър-председателя, състои се от осем членове на правителството (двама заместник министър-председатели, министрите на отбраната, външните работи, вътрешните работи, финансите, промишлеността и търговията и здравеопазването), както и ръководителя на администрацията на държавния материален резерв, управителя на чешката народна банка и секретаря на правителствения кабинет. [3]

Към съвета функционират четири комисии: [3]

- *Комисия за координация по външна политика и сигурност.* Председателства се от министъра на външните работи, координира външната политиката за сигурност на ЧР и отношенията с международните организации за сигурност;
- *Комисия по планиране на отбраната.* Председателства се от министъра на отбраната, координира планирането на мерки за осигуряване на отбраната на страната;
- *Комисия за аварийно планиране.* Председателства се от заместник-министърът на вътрешните работи (който е и директор на националната противопожарна и спасителна служба), планира мерки и координира изисквания към гражданските ресурси за обезпечаване на вътрешната сигурност на държавата, гражданите, икономика и критичната инфраструктура;
- *Комисия за разузнавателната дейност.* Председателствана от министър-председателя, подготвя документи от разузнаваните източници, отнасящи се до сигурността на страната и дейността на разузнавателните служби.

Централният кризисен щаб е работен орган на правителството на ЧР, отговарящ за управлението при кризи.

Щабът е отговорен за оперативното координиране, мониторинга и оценката за изпълнението на мерките, приети от правителството, министерствата и другите административни органи за предотвратяване и/или справяне с възникнали кризисни ситуации, както и осигуряване на подкрепа за дейностите, извършвани от органите за управление при кризи на регионално и местно ниво. [5] В допълнение: [5]

- отговаря за оперативната координация на мерките, прилагани от административните власти, регионалните и местни органи на изпълнителната власт;
- отговаря за оперативно сътрудничество с органите за управление на извънредни ситуации на международни организации;
- отговаря за оценката при развитието на конкретната ситуацията, съдържанието и адекватността на мерките, приети от административните власти, регионалните и местни органи на изпълнителната власт, предоставя информация на Съвета за национална сигурност;
- оценява, обсъжда и координира приемането на мерки от междуведомствен характер, предложени от отделните министерства;
- изготвя, за Съвета за национална сигурност, проекти на мерки за управление на възникнали кризисни ситуации и съответната документация за приемането

на решения, които изискват одобрението на правителството или одобрение от страна на парламента на ЧР.

Централния кризисен щаб се свиква от премиера на страната. Председателства се от министъра на вътрешните работи или министъра на отбраната. Състои се от тридесет и шест члена. [5]

За управление при кризи на регионално равнище (наводнения, големи транспортни произшествия, епидемии, пожари, екологични бедствия) се свикват *регионални кризисни щабове.* В техните правомощия влиза обявяването на извънредно положение на регионално ниво. Председателстват се от ръководителя на региона. В структурата им влизат ръководителите на съответните териториални противопожарни и полицейски сили. [3]

За управление при кризи на общинско ниво се свикват *местни кризисни щабове.* В техните правомощия влиза обявяването на извънредно положение на територията на общинската единица. Председателства се от кмета на общината. В структурата му влизат представители, по аналогия с регионалните кризисни щабове, на общинско ниво. [3]

С цел координация на действията на органите за сигурност на държавата е създадена *Интегрирана спасителна система.* Председателства се от ръководителя на Националната противопожарна и спасителна служба (който е и заместник министъра на вътрешните работи). Системата се задейства по време на кризи в рамките на страната, или в чужбина (след одобрение от правителството). Системата се използва в отговор на всички видове кризи от невоенен характер, по предварително изготвени оперативни планове. [3]

- Интегрирана спасителна система включва следните основни компоненти:
- Противопожарната и спасителна служба;
- Полицейски сили;
- Службата за бърза медицинска помощ;
- Специализирани звена на чешката армия;
- Специализирани спасителни служби (минна спасителна служба, планинска спасителна служба, спелеолози и др.)

Процесът по управление при кризи в ЧР включва: [3]

1. Постъпване на информация и нейната първоначална оценка от оперативния център.
2. Активиране на механизмите за отговор при кризи (свикване на кризисни щабове на съответното ниво – държава, регион, община). Включване на ресурси от всички необходими институции и органи за справяне със съответната ситуация.
3. Разгръщане на адекватни сили и мерки.
4. В случай на необходимост създаване на специализирани екипи за решаване на възникнали отделни проблеми.
5. Информиране на обществеността.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:
1. Павлов, Н., Мястото на България в Европейската система за управление при кризи, С., 2012.
2. Fire rescue service of the Czech republic. Crisis management in the CR. 2013, HZCR, <http://www.hzscr.cz>.
3. Kosek, M., „Crisis Management in the Czech Republic“. Whole-of-Government Course on Security Sector. Governance and Oversight, Session IIIB - Crisis Management, O., 2009, DCAF, <http://www.dcaf.ch>.
4. Government of the Czech Republic. Activities of the Office of the Government : National Security Council. 2013, <http://www.vlada.cz>.
5. Government of the Czech Republic. Activities of the Office of the Government : Central Crisis Staff, 2013, <http://www.vlada.cz>.

ПОЛИТИКИ НА СЪЕДИНЕНИТЕ АМЕРИКАНСКИ ЩАТИ ПРИ УПРАВЛЕНИЕ НА КРИЗИ

Здравко Ю. Кузманов

Шумен ул. „Карел Шкорпил” 1 Факултет „Артилерия, ПВО и КИС”

POLICIES OF THE UNITED STATES OF AMERICA IN CRISIS MANAGEMENT

Zdravko Y. Kuzmanov

Shumen, 1 Karel Shkorpil Str., Faculty of Artillery, Air Defence and CIS

KEY WORDS: *United States, Crisis Management, policies.*

Исторически, правителството на САЩ на всички нива – местно, щатско и федерално има водещата роля в управлението при кризи. Противопожарните и полицейски служби на местно ниво, както и Националната гвардия на федерално ниво, носят основната тежест при овладяването на кризисни ситуации.

С цел координиране на комуникацията по време на фазата на реагиране при криза, *Федералната агенция за управление на извънредни ситуации* (Federal Emergency Management Agency – FEMA) в рамките на *Министерството на вътрешната сигурност* (Department of Homeland Security) администрира *Националния план за реагиране* (National Response Plan – NRP). Този план е предназначен за интегриране на публичният и частният сектори, като очертава общата рамка за отговор при извънредни ситуации. Основава се на предпоставката, че при извънредни ситуации трябва да се работи на най-ниското възможно ниво. *NRP*, признава частния сектор, като ключов партньор във вътрешното управление на инциденти,

по-специално в областта на защитата на критичната инфраструктура и след кризисното възстановяване. [1]

В *NRP* е спътник на Националната система за управление на инциденти (National Incidence Management System – NIMS), която действа като единен общ модел за управление на инциденти, независимо от причината, размера или сложността. [1]

Федералната агенция за управление на извънредни ситуации, се явява основният орган за комплексно решение на проблемите свързани със защитата на националните интереси в кризисни ситуации. [2]

Задачите на *FEMA* включват: [3]

- обезпечаване на защитата и безопасността на населението и ресурсите на страната;
- ликвидация на последствия от стихийни бедствия, крупни промишлени катастрофи и транспортни аварии
- прогнозиране и предотвратяване на извънредни ситуации.

Въпреки че е включена в набора от основни задачи, *FEMA* не е ангажирана основно с предупреждаване за потенциални извънредни ситуации, а с ликвидацията на последиците, разработване на планове и програми за действие в случай на възникване, програми за създаване на стратегически запаси, осъществяване на контрол за съответствие на плановете на различни организации. *FEMA* оказва помощ на ръководствата на отделните щати и органи на местната власт при планирането на действия в случай на възникване на извънредна ситуация от всякакъв тип, определя конкретните им задачи. Агенцията се явява основна и съставна част на националната система за управление на развитието на страната. Образувана е на основата на четири федерални ведомства – министерствата на отбраната, жилищното и горско развитие, търговията, административни органи за общо обслужване с предаване на част от техните функции, а също и отделни функции от кабинета на президента на САЩ.

Цялата територия на страната е разделена на 10 региона, всеки от които е на пряко подчинение на *FEMA* относно въпросите касаещи обезпечаването на готовността на държавните органи и населението в случай на крупномащабни катастрофи и бедствия. Съответно функционират 10 регионални центъра на агенцията. Тези центрове се използват за поддържане на непосредствени контакти, както с местните власти, така и с обществени организации.

Директорът на *FEMA* е пряко подчинен на президента на САЩ и в своята работа осъществява тясно сътрудничество с Националния съвет за сигурност, Кабинета на министрите и Белия дом. В случай на възникване на извънредна ситуация, агенцията обезпечава централизираното ръководство и координацията на спасителните и възстановителните операции, нормалната работа на средствата за комуникация, поддържането на единна база данни за хода на операциите, оказва необходимата помощ на местните органи за управление.

При обявяване на извънредна ситуация директорът на Агенцията назначава оператор по федерално координиране, който ръководи водещите мероприятия и координира всички действия на централната власт и помощните организации. В района на бедствието се организира команден пункт и съгласуване на място про-

веждането на необходимите мероприятия с координатора на щата, представляващ администрацията на последния и осъществяващ контактите с общинските единици.

За изпълнение на всички необходими мероприятия на местно ниво се привличат специални формирования на съответния щат, полицейски, противопожарни, медицински служби, националната гвардия, обществени формирования и граждански сили. При ситуация в която тези сили за борба с бедствието и ликвидацията на неговите последствия са недостатъчни, *FEMA* може да привлече сили на министерството на отбраната. В тези случаи за комуникация и съгласуване на действията на агенцията и командващия континенталната част на страната в съответния регион, се назначава оперативен координатор на всички провеждани военни мероприятия.

Както в мирно, така и във военно време органите на *FEMA* имат право, при извънредни обстоятелства, да използват оборудване, установки и ресурси на министерството на отбраната. Агенцията поддържа постоянна комуникация с центъра на военното командване и родовете войски ВВС, ВМС и сухопътни войски (например, за евакуация на хора – с оперативния център на ВВС). Поддържа се и непрекъсната връзка със Северноамериканския команден пункт на войските за ПВО, както и с щабовете на различните войскови части, в случай на необходимост от оказване на помощ за гражданските власти по време на бедствие. *FEMA* взаимодейства с НАТО и органите за управление при извънредни ситуации на Канада и Мексико, при планиране на съвместни действия в случай на възможни бедствия от национален мащаб. При извънредното планиране, структурите на агенцията привличат управленията на противопожарната охрана, полицията и комуналните услуги, като осъществяват оперативната координация между тях

Органите на *FEMA* организират своята работа в съответствие с концепцията за обединеното управление на страната при извънредни ситуации, която се заключава в създадената в САЩ интегрирана система за управление при извънредни ситуации (Integrated Emergency Management System – IEMS). [3] Една от целите на тази система за управление се явява обединението на съществуващите програми за обезпечаване на готовността, осъществявани във агенцията, други федерални ведомства, органите за управление на щатовете, местните юридически и частни предприемачески организации. Друга цел се заключава в обезпечаване на ефективното използване на ресурси в извънредна обстановка.

Възможностите на *FEMA* както за перспективно планиране, така и за реализация на работните програми в значителна степен зависят от организацията на комуникациите и автоматизираната обработка на данните. За тази цел е създадена Национална система за управление при извънредни ситуации (National Emergency Management System – NEMS), [3] която се състои от средства за комуникация, информационна система и различни средства за обслужване.

NEMS представлява сложен механизъм, предназначен за събиране, обработка и разпределение на информация в интерес на организацията на действията в извънредни ситуации на федерално, щатско и местно ниво. За осъществяване на връзка и управление при президента вицепрезидента и директора на агенцията е създаден информационно-координационен център за действия в условията на извънредни ситуации. Благодарение на него е възможно изпълнението на функциите на *FEMA*, като централен орган, чрез който комуникират всички правителствени органи на изпълнителната власт, отговорни за предоставяне на целият обем необходима информация към ръководителя на действията при извънредни ситуации в различен мащаб. [2]

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. Federal Emergency Management Agency. Quick Reference Guide for the National Response Plan (version 4.0). 05.2006. 2013, FEMA, <www.fema.gov>.
2. Владимиров В., Малинецкий Г., Потапов А. и кол. Управление риском. Риск. Устойчивое развитие. Синергетика. Наука, М., 2000.
3. Federal Emergency Management Agency. FEMA. 2013, < www.fema.gov >.

ИНФОРМАЦИОННА СИГУРНОСТ

МОДЕЛ ЗА ОЦЕНКА НА ВЪНШНАТА СРЕДА ПРИ АНАЛИЗА НА КОРПОРАТИВНИЯ РИСК

Румен Ст. Гюров

град София 1505, улица „Черковна“ № 90, Държавна комисия по сигурността на информацията, имейл: dksi@governmet.bg, gyurov.rumen@gmail.com

ASSESSMENT FRAMEWORK FOR EXTERNAL ENVIRONMENT IN CORPORATE RISK ANALYSIS

Rumen St. Gyurov

ABSTRACT. *The accepted corporate risk analysis standards do not provide well-organized tools for their successful implementation. Therefore there is a need to developing a comprehensive analytic model for assessing the environment.*

KEY WORDS. *Corporate governance, external environment, risk analysis.*

Анализът на корпоративния риск предизвиква интерес, както заради формалната асоциативна връзка с финансовите мащаби на корпоративния бизнес, така и заради риска, който всеки се стреми да избегне. Разбираемо е, че човешкото внимание е привлечено от материалната мощ на парите и несигурността на утрешния ден. Несигурността бе ярко демонстрирана с финансовата криза от 2008 г. Оказа се, че в глобалния свят дори мощните транснационални корпорации са уязвими. Още в първата година на кризата 85% от тях изпитаха значителни трудности и намалиха своите преки задгранични инвестиции [1]. Спадът на преките чуждестранни инвестиции тогава доведе в най-добрия случай до стагниране на националните икономики впоследствие. И неслучайно финансовата криза засегна 78 млн. души по света [2]. Можеше ли кризата да бъде избегната? Как да преодолеем днешните й негативни последици? Може ли тя да се възпроизведе в бъдеще? Отговорът на изразената с тези въпроси тревога лежи в изчерпателното обяснение на скритите й причини и механизми. Обяснението им безспорно е обект на анализ на риска, а външната среда, чиято динамика предопределя бизнеса на компаниите и развитието на икономиката въобще, представлява приоритетен предмет на изследване. Но задачата тук не е обяснение на кризата от 2008-а, а разработване на подходящ аналитичен модел. Затова структурирането на анализа на корпоративния риск и особено структурирането на анализа на външната среда представлява заслужаващо си усилията интелектуално и практическо предизвикателство.

Първият стандарт за управление, вкл. анализ, на риска се появява в Норвегия през 1991 г. Впоследствие се появяват и други, например – британският стандарт за управление на проектния риск от 2000 г. [3]. С добре разработени стандарти за управление на риска, вкл. корпоративния, разполагат Великобритания, Канада, Австралия, Нова Зеландия и други страни от Г-20. Всички стандарти имат за цел да осигурят съгласуваност в управлението на риска и във всички тях присъстват компонентите на анализа на риска. Макар терминологията им да варира, общо остава разграничението между преценка (risk estimation) и оценка на риска (risk assessment). Първото представлява заключение за вероятността и последиците от риска; второто – за въздействието на риска върху вземането на решения [4].

Само че отзивите за съществуващите методологии никак не са ласкави: „[...] нито едно от съществуващите ръководства за управление [вкл. анализ] на риска не е адекватно за целта си. Повечето от ръководствата са на изключително високо равнище [респективно, енигматични за разбиране и сложни за употреба], ориентирани са спрямо процесите и дават твърде оскъдни указания как да бъдат създадени ефективно управление на риска и осигурителна рамка [5].“ Според мен най-съществените причини за неласкавите отзиви се изразяват в това, че:

1. Различните стандарти тръгват от частни случаи, като особеностите на тези случаи се пренасят върху всички случаи въобще [6].

2. Определенията за риска са лошо формулирани, при което всяко негативно явление се включва в категорията „риск“.

3. Акцентът се поставя повече върху вътрешната среда и т. нар. оперативни рискове, отколкото върху външната среда и т. нар. стратегически рискове [7].

4. Многообразието от аналитични методи и техники не се систематизира на рационална основа, а по различни признаци и в разнопосочни таксономии, без единна концептуална обосновка. Все пак повечето стандарти, ръководства и разработки се обединяват около методи като: регистър на рисковете, дърво на събитията, дърво на решенията, дърво на грешките; вероятностни техники, вкл. симулация „Монте Карло“; експертни методи като чек-листи, интервюта, мозъчна атака, метод „Делфи“, анализ по сценарии и др. Но дори тези общоприети методи и техники не се поставят еднозначно, на строго определено за тях място в аналитичния процес [8].

Многообразието от гледни точки и разработки е впечатляващо, ако се вземе предвид представителна извадка от Световната библиотека „Интернет“, но вместо да улесни, то затруднява избора на подходяща методология заради посочените слабости. Обърквашото многообразие на предимно англоезичната Мрежа се сменя от еднозначно и недостъпно, концептуално и институционално мълчание в българския й сектор. Търсенето с ключови думи „корпоративен риск“ в Google дава едва 17 300 резултата в сравнение 1 380 000 резултата за ключовите думи “corporate risk” към дата 25 май 2014 г. Преобладаващото мнозинство български резултати е свързано със сайтове като „Помагало“ (www.pomagalo.com) и „Реферати“ (www.referati.org), за които смятам, че не се нуждаят от представяне. Останалите резултати могат да бъдат открити в „административни“ файлове на някоя банка или висше училище, които по същество не предлагат визия за анализ и оценка на риска.

В този контекст погледът към българската нормативна база не носи изненада. В търсенето на корпоративния риск закони като тези за Българската народна банка, Комисията за финансов надзор, корпоративното подоходно облагане и пазарите на финансовите инструменти не предлагат определение за риск, корпоративен риск и

под. [9]. Споменават се производни понятия като кредитен, ликвиден и лихвен риск [10]. Тези понятия не са нормативно определени вероятно поради факта, че съдържанието им е азбучно известно в икономическата наука. Спорадично се откриват нормирани определения на понятията системен и операционен риск [11]. Тоталната липса на определение за понятието риск или дори липса на самото понятие изненадва в специализирани закони като тези за Министерството на вътрешните работи, отбраната и въоръжените сили, защитата на класифицираната информация, Държавна агенция „Национална сигурност“ [12]. Подобна е картината и в други български закони със сходно или близко приложно поле [13]. Българското законодателство все пак асоциира риска с „вероятността от възникване на неблагоприятни последици или изменения“ за здравето и безопасността на хората, което е изключително близко до широко приетите определения за риск [14].

Очевидно е, че изходът от подредения хаос и аналитичния вакуум е някъде другаде. В разширен контекст на търсене външната среда се структурира на две основни равнища, всяко от които е предмет на ясно разграничен спектър от аналитични методи и техники:

– Макроравнище на културната, социалната, политическата, правната, регулаторната, финансовата, технологическата, икономическата, природната или/и международна, национална, регионална или/и локална среда на обществения живот (с използване на анализ от типа TEMA, STEEP, PESTI и пр. анализ);

– Микроравнище на непосредствената оперативна среда на даден бизнес, която се характеризира с: пазарна и потребителска сегментация (тогава имаме съответния анализ на пазарната и на потребителската сегментация), отраслови особености, въздействия от т. нар. Пет сили на Портър, конкуренция, благоприятни фактори за постигане на успех, заинтересувани страни [15] и пр.

Някои обособяват равнище на максимална неопределеност, неизвестна среда с непознати източници на риск, наречена „Син океан“. Равнищата с по-голяма определеност са обединени в понятието „Червен океан“ и спрямо тях се прилагат стандартни методи и техники. Аналитичният подход към „Син океан“ е структуриран около отговорите на четири основни въпроса: 1. Влиянията на кои фактори трябва да бъдат отстранени? 2. Влиянията на кои фактори трябва да бъдат минимизирани? 3. Влиянията на кои фактори трябва да бъдат стимулирани? 4. Влиянията на кои фактори и какви фактори трябва да бъдат създадени [16]? Отговорите на тези четири въпроса снемат практически всяка неопределеност независимо от равнището на структуриране на средата. Тяхното поставяне може да бъде отправна точка в подбора на подходящи методи и техники въобще.

Критериите за избор на аналитични методи и техники включват изискванията: първо, методите да са консистентни (съответстващи на ситуацията), повторими, проверими и верифицируеми; второ – да са способни да изградят достоверно разбиране за конкретния риск [17].

Началната стъпка към такова разбиране е формулирането на смислено определение. Рискът може да бъде дефиниран като нарушено равновесие между дадена система (корпорация, организация, държава, общност, нация, човек...) и нейната среда в резултат от неблагоприятно въздействие при недостиг на ресурс за съхраняване на системата. Рискът е конкретно съотношение между събития и последици. Може да се появи във всяка област: финанси, производство, здравеопазване, околна среда, обществен ред... [18] Конкретизацията на това определение е след-

ващата стъпка, която включва самото идентифициране, ранжиране, картографиране и корелиране на действителните, потенциалните и остатъчните рискове [19]. Целта е преценка на нивото на риска: силата на неговото въздействие и вероятността на последиците от него [20].

Неразделна част от определянето на риска е предварителното селектиране на външния и вътрешния контекст чрез подбор на показателите, критериите и обхвата на риска [21]. Съгласно актуалния днес стандарт ISO 31000:2009 „основните елементи на външния контекст включват широката културна, социална, политическа, правна, регулаторна, финансова, технологическа, икономическа, природна и конкурентна среда, както и възприятията и ценностите на външните заинтересувани страни“ [22]. Сходни разграничения във вижданията за измерване на националната сила редуцират средата до няколко значими области: дипломация, информация, военно дело, икономика – DIME (от абревиатурата на наименованията на латиница), или политика, военно дело, икономика, общество, инфраструктура, информация – PMESII и др. [23]. Въз основа на обективирана йерархия на потребностите, тези области могат да бъдат сведени рационално до икономика (интереси за оцеляване, придобиване на ресурс), общество (интереси за безопасност, достъп до ресурс), култура (интереси за сътрудничество при усвояване на ресурс) и управление (интереси за контрол върху потребяването на ресурс), обозначени на латиница с EPSC [24]. И това е първата ни реална стъпка към търсения модел!

„Моделите за измерване [анализ и оценка] са формативни или рефлективни. Разграничението помежду им се извършва според посоката на причинно-следствената връзка между латентните променливи и техните индикатори. Докато формативните модели показват, че индикаторите са наблюдаемите променливи, които причиняват латентните, то рефлективните показват, че латентните променливи причиняват наблюдаемите и по такъв начин са измерими [25].“

Ако трябва да бъдат сумирани вижданията дотук, един рационален модел е необходимо:

– да обхваща изчерпателно контекста, в който се идентифицират, ранжират, картографират и корелират рисковете (съобразно поставените тук цели моделът е ограничен само до външната среда);

– да е съобразен с равнищата на анализ, разграничени с оглед адекватна оценка на риска и неговите последици;

– да съчетава характеристиките на формативните и рефлективните модели, като предлага ясна подредба на видовете рискове с цел използването на адекватни за тях аналитични методи и техники;

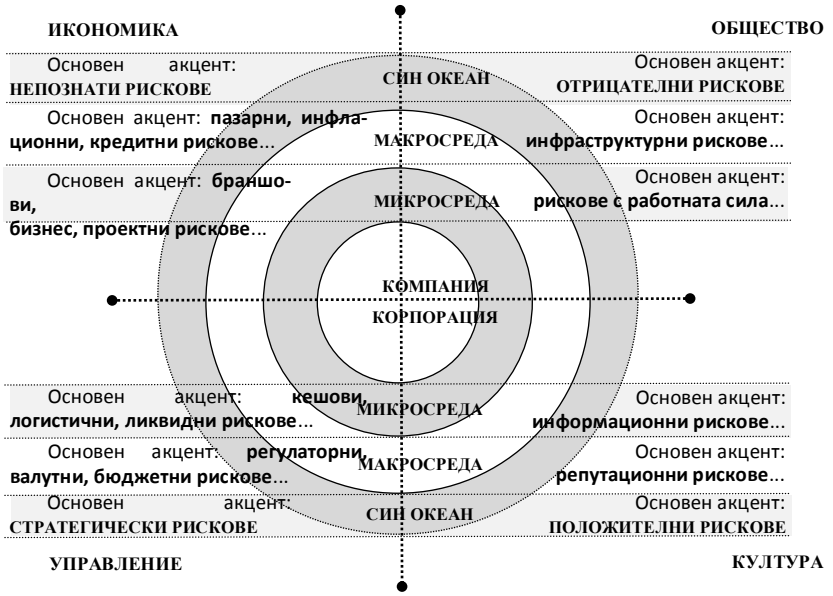
– да е рационално обоснован, като свежда многообразието от разграничения до относително опростена структура на средата.

Съобразно приетите определения, разграничения, вложен смисъл и логика на използвания подход, рационалният модел (вж. фиг. 1) на външната среда при анализа на корпоративния риск разделя стратегическия контекст на четири сектора – икономика, общество, култура и управление, и на три равнища: „Син океан“, макросреда и микросреда.

На равнище „Син океан“ са обособени рисковете с най-голямо влияние върху определяне на стратегиите за преодоляването им в съответния сектор от средата. Независимо от сектора на приложение, на това хиперравнище най-подходящи

аналитични методи и техники са: методът на двете оси, методът на конуса на правдоподобността, мултифакторният анализ; анализът по сценарии [26] и пр.

ФИГ. 1. МОДЕЛ ЗА ОЦЕНКА НА ВЪНШНАТА СРЕДА И КОРПОРАТИВНИЯ РИСК



По идея от: Jachia and Nikonov (2012: 27) и Strategic… (2007: 32–33).

На макроравнище най-подходящи за използване в икономически аспект са методи и техники като: анализ на пазарната, технологичната, потребителската, продуктовата сегментация; в обществен аспект – анализ на критичната инфраструктура (транспортна, комуникационна, демографска, социална, социокултурна и пр.); в социетален аспект – социокултурен анализ (анализ на убеждения, стереотипи, ценности и поведение); в управленски аспект – правен, регулаторен, институционален, фискален анализ [27] и др.

На микроравнище препоръчителни за използване в икономически аспект са: браншовият и конкурентният анализ, аналитичната матрица на петте сили на Портър (анализ на новите конкуренти, продуктите-заместители, покупателната способност, снабдяването и конкурентните взаимодействия), анализът на заинтересуваните страни и пр.; в обществен аспект – анализ на социалното и здравното осигуряване и онези методи и техники, които са свързани с оценката на състоянието на работната сила; в социетален аспект – анализ на репутационния риск; в управленски аспект – анализ на управлението на кешовите потоци, снабдяването и ликвидността [28].

Особеност на предложения модел е, че аналичните методи и техники, препоръчително приложими на „по-високо“ равнище („Син океан“), могат да бъдат прилагани и на съответното „по-ниско“ равнище (респ. макро- и микросреда).

Внимателният прочит на модела за оценка на външната среда и корпоративния риск показва: първо, спецификата на риска като съотношение и произтичащата от него необходимост за анализ на вътрешната среда (организационната среда на компанията, корпорацията...); второ, потребността от категорично разграничаване на методите от техниките за анализ с оглед мястото им в аналитичния процес. Затова:

Първо. Прави впечатление, че всеки от изброените в модела рискове е съотносим към състоянието на вътрешната среда. Например браншовият анализ задължително трябва да бъде придружен от анализ на същностните способности на компанията, а цялостният анализ на средата (и външна, и вътрешна) следва да бъде допълнен с помощта на популярния SWOT-анализ, разширен от т. нар. ACT-ON-анализ (включващ освен силни и слаби страни, възможности и заплахи, също и следващи стъпки, необходими за развитието на компанията) [29].

Второ. Разграничителната линия между методи и техники за анализ може да се очертае въз основа на следното разбиране: метод от типа на посочените по-горе е познавателно средство за обособяване и структуриране на предметното поле на анализа (напр. браншови анализ, т. е. анализ на конкретния бранш, отрасъл); техника от типа на посочените по-горе е организационно средство за интегриране на експертните оценки на различни анализатори на риска, независимо от използвания от тях метод (напр. чек-листове, интервюта, мозъчна атака, метод „Делфи“ и пр.). В този смисъл методите са приложими най-успешно на определено аналитично равнище, в определено предметно поле на анализа, а техниките – на всички равнища.

Направените уточнения по отношение на предложения модел спомагат за по-доброто разбиране на евристичната му сила. Моделът подсказва възможности за своето бъдещо развитие чрез включване на вътрешната среда в него и по-нататъшно интегриране на методите и техниките в аналитичния процес.

БИБЛИОГРАФСКИ БЕЛЕЖКИ

[1] World Investment Report 2009: Transnational Corporations, Agricultural Production and Development. Overview. United Nations: New York and Geneva, 2009, http://unctad.org, wir2009overview_en, PDF, 25.05.2014, p. 9.

[2] Младенова, Марта. 78 млн. души са засегнати от глобалната финансова криза, 17.09.2009 г., http://dariknews.bg/view_article.php?article_id=401444.

[3] Fineman, Milijana. Improved Risk Analysis for Large Projects: Bayesian Networks Approach. Queen Mary, University of London, 2010, https://qmro.qmul.ac.uk, 18.04.2014, PDF, p. 18.

[4] Fineman, M. Improved…, p. 19.

[5] Anderson, Richard, et al. Risk Management and Corporate Governance. OECD, 30.04.2009, www.oecd.org, 18.04.2014, PDF, p. 3.

[6] Вж. Fineman, M. Improved…, p. 20 etc.

[7] Anderson, R., et al. Risk…, p. 14.

[8] Срв. Damodaran, Aswath. Risk Management: A Corporate Governance Manual. New York, 2010, http://people.stern.nyu.edu, 18.04.2014, PDF, p. 29–32, etc.; Fineman, M. Improved…, p. 29–38, 49–59; Risk Management – Risk Assessment Techniques.

International Standard IEC/FDIS 31010:2009(E). Final Draft. Brussels, 2009, www.previ.be, 18.04.2014, PDF, p. 29–91; Van der Laan, Lucas. Foresight Competence and the Strategic Thinking of Strategy-level Leaders. Toowoomba, University of Southern Queensland, Australia, 2010http://eprints.usq.edu.au, 24.01.2012, PDF, p. 195–214.

[9] Вж. Закон за Българската народна банка (ЗБНБ), Закон за Комисията за финансов надзор (ЗКФН), Закона за корпоративното подоходно облагане (ЗКПО), Закона за пазарите на финансовите инструменти (ЗПФИ) и др.

[10] Напр. чл. 20, ал. 2 ЗБНБ ; чл. 42, ал. 1, т. 3 ЗКИ; § 1, т. 32 ДР ЗКПО; чл. 3, т. 2, б. ж ЗПФИ и др.

[11] Напр. § 1, т. 32 и 45 от Допълнителните разпоредби (ДР) на Закона за кредитните институции (ЗКИ).

[12] Вж. Закон за отбраната и въоръжените сили на Република България (ЗОВС), Закон за защита на класифицираната информация (ЗЗКИ), Закон за Държавна агенция „Национална сигурност“ (ЗДАНС), Закон за Министерството на вътрешните работи (ЗМВР). Понятието риск е споменато мимоходом три пъти в чл. 74а и 213, ал. 1 и 3 ЗМВР, два пъти в § 45 от Преходните и заключителни разпоредби (ПЗР) на ЗОВС, само един път в § 1, т. 14, б. д ДР ЗЗКИ и въобще не е споменато в ЗДАНС (ако не броим неясното, и което не е същото, „рискова дейност“ в чл. 101, ал. 1 ЗДАНС).

[13] Вж. напр. Закон за безопасно използване на ядрената енергия (ЗБИЯЕ), Закон за експортния контрол на продукти, свързани с отбраната, и изделия и технологии с двойна употреба (ЗЕКПСОИТДУ), Закон за мерките срещу изпирането на пари (ЗМИП), Закон за мерките срещу финансирането на тероризма (ЗМФТ).

[14] Чл. § 1, т. 4 и 5 от ДР на Закона за здравословни и безопасни условия на труд (ЗБУТ).

[15] Strategic Management Toolkit. Handbook. From Mission to Action Management Series for Microfinance Institutions. Warsaw, Microfinance Centre for Central and Eastern Europe and the New Independent States, March 2007, http://inthiseconomy.org, 14.02.2013, PDF, p. 31. Вж. също Risk Management – Principles and Guidelines. Indian Standard (ICS 03.100.01). New Delhi: Bureau of Indian Standards (BIS), 2011, https://law.resource.org, 18.04.2014, PDF, p. 19, 24; Kruger, Jean-Pierre. A Study of Strategic Intelligence as a Strategic Management Tool in the Long-term Insurance Industry in South Africa. Univer-sity of South Africa, January 2010, http://uir.unisa.ac.za, 14.02.2013, PDF, p. 25–28, 68–69; Rhydderch, Alun, et al. Scenario Planning. Guidance Note. Foresight Horizon Scanning Centre, Government Office for Science, October 2009, www.bis.gov.uk, 14.02.2013, PDF, p. 11–13; Zegers, Robert, and Cornelius Murombezi. Strategic Management. Jordanian Edition. Adapted by Mahmoud al-Sayyed. Amman, The Hashemite Kingdom of Jordan, 2004, ISBN 9957-447-06-8, http://pdf.usaid.gov, 14.02.2013, PDF, p. 22–28.

[16] Isoherranen, Ville. Strategy Analysis Frameworks for Strategy Orientation and Focus. Oulu, Finland, University of Oulu, Faculty of Technology, Department of Industrial Engineering and Management, 2012, http://herkules.oulu.fi, 14.02.2013, PDF, p. 34–36.

[17] IEC/FDIS 31010:2009(E), p. 20.

[18] Срв. AS/NZS ISO 31000:2009, p. 9; ICS 03.100.01, p. 10–11

[19] Вж. Shenkir, William G., and Paul L. Walker. Enterprise Risk Management: Tools and Techniques for Effective Implementation. Montvale, NJ, USA: Institute of Management Accountants, 2007, http://erm.ncsu.edu, 18.04.2014, PDF, p. 15.

[20] ICS 03.100.01, p. 15.

[21] ICS 03.100.01, p. 12; IEC/FDIS 31010:2009(E), p. 11–12.

[22] Jachia, Lorenza, and Valentin Nikonov. Risk Management in Regulatory Frameworks: Towards a Better Management of Risks. United Nations: United Nations Economic Commission for Europe, New York – Geneva, 2012, www.unece.org, 18.04.2014, PDF, p. 26.

[23] Elements of National Power. Bibliography. Joint Forces Staff College – Ike Skelton Library. Norfolk, Virginia, USA, www.jfsc.ndu.edu, 01.12.2013, PDF, 28 p.

[24] За обективирането на потребностите вж. Лазаров, Валери, и Румен Гюров. Матрични решения за националната сигурност. София: Издателство „Изток-Запад“, 2012, с. 36–38.

[25] Van der Laan, L. Foresight…, p. 158–159.

[26] Срв. Rhydderch, A., et al. Scenario…, p. 11–12.

[27] Срв. Jachia, L., and V. Nikonov. Risk..., p. 27 etc.; Strategic…, p. 32.

[28] Срв. Kruger, J.-P. A Study..., p. 27; Rhydderch, A., et al. Scenario…, p. 11; Shenkir, W. G., and P. L. Walker. Enterprise..., p. 15; Steinberg, Richard M., et al. (PricewaterhouseCoopers LLP). Enterprise Risk Management – Integrated Framework: Application Techniques. Committee of Sponsoring Organizations of the Treadway Commission (COSO), September 2004, www.macs.hw.ac.uk, 26.04.2014, PDF, p. 40, 54–55; Strategic…, p. 32.

[29] Shenkir, W. G., and P. L. Walker. Enterprise..., p. 10–11; Zegers, R., and C. Murombezi. Strategic..., p. 38–40; ACT-ON. A Tool for Assessing Your Environment and Creating an Initial Strategic Plan. Adapted from Cohen, David; de la Vega, Rosa, and Watson. Advocacy for Social Justice: A Global Action and Reflection Guide, Chapter 2, Kumarian Press, Inc., Connecticut, USA, 2001, http://internationalbudget.org, 14.02.2013, PDF, p. 1–2.

СТЕГАНОЛОГИЧНА ЗАЩИТА НА ИНФОРМАЦИЯТА В КОНТЕКСТА НА КОНТРАРАЗУЗНАВАТЕЛНОТО ОСИГУРЯВАНЕ НА СИГУРНОСТТА НА ВОЙСКОВИ КОНТИНГЕНТ ЗАД ГРАНИЦА[1]

Калин И. Кръстев

Университет по библиотекознание и информационни технологии , гр. София

Станимир С. Станев

Шуменски университет „Епископ Константин Преславски”

STEGANOLOGICAL PROTECTION OF THE INFORMATION IN THE CONTEXT OF COUNTERINTELLIGENCE ENSURE THE SECURITY OF MILITARY CONTINGENT ABROAD

Kalin I. Krastev

University of library studies and information technologies, Sofia

Stanimir S. Stanev

Shumen University “Bishop Konstantin Preslavski”

ABSTRACT: *Revealed the threat to confidentiality of the information of military contingent abroad through the use of recent achievements in computer steganography. Is modeled stegokanal for flowing of the information. Based on counterintelligence principles for protection of the information are proposed directions and measures for steganological protection.*

KEY WORDS*: steganology, computer steganography, counterintelligence, protection of the information.*

Целта на всяка автоматизирана информационна система (АИС) е предоставяне на пълна, достоверна и своевременна информация. В реалните условия на действие на наши войскови контингенти зад граница, тази информация е уязвима, както поради случайни, така и поради злонамерени дестабилизиращи фактори (заплахи). Това налага да се вземат мерки за нейната защита, чрез които се постига нужното ниво на информационна сигурност. Основните мерки за защита на конфиденциалната информация в БА и нейните войскови контингенти се базират на съответните закони, наредби и правилници [1,2].

[1] Разработката е частично финансирана от фонд „Научни изследвания” на Шуменския Университет „Епископ К.Преславски” по проект РД 08-248 / 2014.

На базата на [3] може да се определи информационната сигурност на войскови контингент зад граница като състояние на защитеност на информационната среда на контингента, при което се осигуряват нейната конфиденциалност, достъпност и цялостност. Според редица специалисти засега липсва технология, която да удовлетворява всички концепции за информационна сигурност [4].

Един от най- важните аспекти на осигуряване на сигурността на АИС е определянето, анализа и класификацията на възможните заплахи за тях. За класифицираната информация в контингента външни преднамерени заплахи могат да бъдат [3]:

- враждебни действия на чуждестранни организации, групи от хора и отделни личности от политически, икономически и разузнавателни структури;
- дейността на международни терористични организации, целяща проникване в информационните системи на военните структури;
- дейността на космически, въздушни, морски, наземни и други технически разузнавателни средства на противникови на контингента държави.

За постигане на своите цели тези организации и групи използват различни методи, включително и нови информационни технологии за информационни атаки [5]. Една от съвременните технологии за скрито предаване на информация е компютърната стеганография. Стеганографията е съвкупност от методи и средства, базирани на различни принципи, които имат една обща цел – скриването на самия факт на съществуването на информация в различни среди [6].

Нарастването на техническите възможности на съвременното разузнаване на терористични и организирани престъпни групи предизвиква необходимостта от адекватни контраразузнавателни технически мерки за противодействие при защитата на информацията на войсковите контингенти зад граница.

Приема се, че стеганография е научно-приложна област, съвкупност от технически умения и изкуство за начините за скриване на факта на предаване (наличие) на информация .От средата на първото десетилетие на XXI век сред специалистите се използва и терминът стеганология, обхващащ два смислово противоположни компонента- стеганография и стеганализ. Под стеганализ се разбират методи и технологии за откриване на скрити комуникации, които използват стеганографски технологии [7].

Въпреки че разследванията в Интернет в началото на това столетие не доказаха възможността терористите да използват високотехнологична стеганография [9], измина доста време, достатъчно те да усвоят такива методи за комуникация. Остаряло е вече и мнението, че инструментите за стеганализ, с който разполагат мощните контраразузнавателни централи, прави много рисково използването на стеганографията от терористи [10] и че е по-вероятно в своите комуникации терористите да използват нискотехнологични методи на стеганографията (нулевите шифри, семаграмите и др.), отколкото високотехнологични стеганометоди. За връзка със своите агенти, службите за сигурност вероятно използват пълен арсенал от средства за стеганографска комуникация за предаване на голям обмен класифицирана информация [11].

В [8] е определено, че стегоинцидент е криминална дейност по използване на компютърната и мрежова стеганография за посегателства към чувствителна информация чрез образуване на скрит канал за изтичане или за несанкциониран достъп до нея.

Канал за изтичане на информацията е метод, позволяващ на нарушител да получи достъп до информацията, обработвана, съхранявана или предавана в системата.

Стеганологичната защита (стегозащита) е комплекс от организационни и апаратно-програмни мерки за предотвратяване на стегоинциденти [8].

Може да се определят два основни аспекта на стегозащитата:

1. Защита на класифицирана информация срещу изтичане с използване на методи на стеганализа.

2. Стегозащита на информацията срещу несанкциониран достъп чрез скриване на конфиденциални данни в безобидни на пръв поглед мултимедийни файлове.

Вторият аспект на стегозащитата не е пряко свързан с контраразузнавателната защита на информацията, и тук само се отбелязва като възможност за използване от службите, осигуряващи предаването на конфиденциалната информация на войсковия контингент.

Система за защита на информацията (СЗИ) е организирана съвкупност на всички органи, средства, методи и мероприятия, предвидени в информационна система за осигуряване на защита на информацията от разгласяване, изтичане и НСД към нея [12].

Тук се приема едно важно ограничение – тъй като СЗИ е комплекс от мерки, реализирани от няколко подсистеми за защита – антивирусна, защитна стена, криптозащита и др., като СЗИ ще се разглежда само подсистемата за стеганологична защита на информацията,състояща се от две части- стеганографска и стеганалитична.

Актуалността на проблема е свързана с отговорностите на службите за сигурност се разкрие опасността от използването на съвременната компютърна стеганография за създаване на канали за изтичане на класифицирана информация от вътрешни за контингента нарушители (т.н. „инсайдери", от англ. insiders) [13] , и да се предложат мерки за ефективно противодействие .

Ролята на защитниците и наблюдателите, още от публикуваната през 1983г. статия на Симънс с „проблема на затворниците" Алис и Боб [14], е все още повече обект на теоретични изследвания, отколкото на практическо приложение. Тук на базата на сценария за Алис и Боб, с цел задълбочено изследване на проблема за възможните стеганографски канали за изтичане на информация, е предложен хипотетичен модел на дейността на разузнавателната служба на престъпна организация „Б" срещу контингента „А" с използване на стеганографски методи (фиг.1). Организацията „Б" поставя задача на разузнавателното си звено да придобие конфиденциална информация от войсковия контингент „А". Изрично е поставено условието задачата да бъде изпълнена в условия на пълна конспиративност, без атакувания контингент да узнае за изтичането на информацията. Разузнавателното звено на „Б" поставя изпълнението на задачата на своя агент „Боб".

От направеното предварително проучване Боб установява, че контингентът „А" има надеждно функционираща система за информационна сигурност, изключваща несанкциониран външен достъп към компютърните му ресурси. Поради това, за изпълнение на тази задача, Боб решава да вербува служител на фирма „А", имащ естествен достъп на база заемана длъжност до желаната разузнавателна информация. След осъщественото изучаване на личния състав на „А", Боб вербува [15] сержант Алис, която отговаря на това условие.

Класифицираната информация, която Алис трябва да предостави на Боб е достъпна само в пункта за класифицирана и некласифицирана информация на контин-

гента. Сведенията, получени от Алис, потвърждават наличието на „твърда" политика за компютърна и мрежова сигурност [6], в контингента „А" и наличието на специализирана стегосистема от типа на StegAlyzerRTS [16] в защитната стена на мрежата на контингента (фиг.1). Предвид съществуващата опасност от разкриване на вербуваният агент Алис, ако тя използва традиционните канали за изтичане на класифицирана информация, Боб търси и намира слабост в системата за сигурност на „А". Това е разрешението за служителите в пункта за класифицирана и некласифицирана информация на „А" да използват не само служебните компютри, контролирани от администратора по сигурността на мрежата на „А"- Вили, но и лични компютри и мобилни апарати за безжична връзка с глобалната мрежа Интернет. Боб решава да приложи стеганографски способи за решаване на задачата. Той осигурява на Алис специално разработена от специалистите на „Б" стеганографска програма „ST" за вграждане на скрити съобщения в мултимедийни носещи файлове (т.н. контейнери), набор от подходящи контейнери и стегоключ (в случая това е съвкупност от правила за установяване на връзка между двамата абонати , вида и парола на използваната програма, начина за вграждане в един или няколко контейнера и др.) , като и адреса на определен от Боб Web-сайт („тайник"), където Алис трябва да изпрати стегограмата със скритата информация. За да не бъде разкрита предварително от Вили за подготовката си за непозволена дейност, Алис може да получи тази информация от облака на фиг.1 - компютри с общи ресурси в Интернет пространството, позволяващи тяхното общо ползване от Алис и Боб.

Основният скрит канал се установява чрез предаване на стего-файла чрез безжичната мрежа до „тайника". Алтернативен скрит канал може да бъде изграден чрез изнасяне на стего във вид на безобиден мултимедиен файл на физически носител. Този вариант обаче е много по- рисков за Алис.

В представената схема (фиг.1) последователността на действия на обект Алис за предаване на класифицираната информация е следната:

След добиване на необходимата информация, Алис изтегля в личния си компютър стегопрограмата и файл- контейнер и използвайки тези средства, преобразува информацията в стегосъобщение. Възможно е тя да използва и алгоритъм за разпръснато вграждане – реализация на времево- пространствен стегометод за вграждане на псевдо-случаен принцип. Възможно е и да се криптира съобщението като втора защита от разкриване, преди неговото вграждане в контейнера [8].

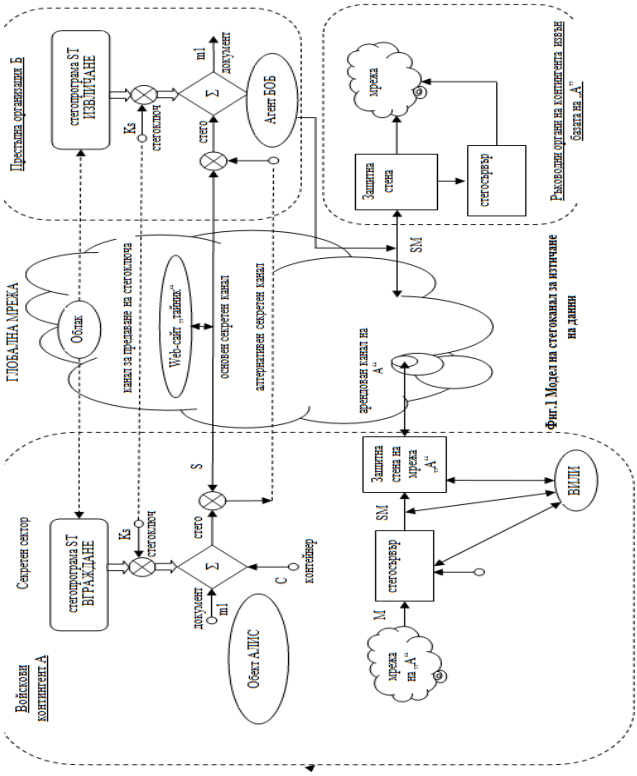
Алис изпраща стегофайла от своя личен компютър чрез безжична мрежа, различна от мрежата на контингента, до посочения от Боб Web-сайт-„тайник". От него впоследствие Боб изтегля стегофайла, чрез уговорените стеганографски средства извлича желаната конфиденциална информация и я предоставя на ръководството на организацията „Б".

След всяко изпращане на стегограма, Алис изтрива всички копрометиращи я файлове от своя личен компютър. Преди всяко следващо предаване тя отново зарежда необходимите и средства чрез облака.

Този сценарий разкрива как на практика чрез използване на методите на стеганографията е възможно конспиративно да бъде извлечена класифицирана информация от войскови контингент, осигуряващо минимизиране на възможностите за нейното разкриване от контраразузнавачите на контингента.

Разкриването на каналите за изтичане на информация и организиране на ефективно противодействие на съществуващите възможности за използване на стега-

нографските методи е основна задача на контраразузнаването на „А” с цел пресичане на престъпната дейност.



Като конкретни мерки за противодействие могат да бъдат посочени [8]:

- забрана на внасянето, качването, тегленето и ползването на криптиращи и стеганографски програми за лични цели ;
- забрана за дотъп до Интернет на компютри, в които се обработва конфиденциална информация, и забрана за презапис на данни върху информационни носители;
- забрана на наличието и внасянето в зоната за сигурност на компютри и мобилни апарати с достъп до Интернет, извън компютърната мрежа на контингента;
- организиране на контрол върху изходящия трафик, чрез проксисървър, защитна стена и др.;
- създаване на междинно звено, обслужващо проксисървъра с възможности за заглушаване на всички свободни интернет услуги;
- създаване на сървър за отстраняване на мултимедийни файлове и ограничаване възможността на служебния канал за прикачване на мултимедийни файлове;

- стеганализ на всички изходящи по официалния мрежов канал на защитавания контингент мултимедийни обекти, предавани в канала или тяхното зашумяване чрез вграждане чрез стегопрограми на специални стеганалитични съобщения, с цел унищожаване на евентуално вградена конфиденциална информация.

За постигане на желаната надеждност и ефективност, задължително условие е съчетанието на горепосочените мерки с класически контраразузнавателни мерки за противодействие [15,17], със спазване на следните принципи на контраразузнавателната защита на информацията на контингента, характеризиращи професионалния подход към тези проблеми:

- съответствие на нивото на защитата на ценността на информацията;
- гъвкавост на защитата;
- многозоналност на разполагане на средствата за защита в зависимост от разположението на източниците на конфиденциална информация;
- многорубежност на средствата за защита на информацията на пътя за движение на вражеския агент (или техническото средство) към източника на конфиденциална информация.

Допълнителен защитен рубеж са и доброволните сътрудници на контраразузнаването [17]. Те се намират в контролираните зони във връзка със своите основни служебни задължения и едновременно с това следят ситуациите. В случай на необходимост веднага уведомяват контраразузнавателния тим за открити нарушения или други значителни факти.

При усъвършенстване на контраразузнавателната система за защита на информацията е целесъобразно освен това да се отчитат и следните принципи:

- минимизация на допълнителните задачи и изисквания към военнослужещите в контингента, обусловени от мерките за защита на информацията;
- надеждност на агентурните и техническите средства, изключващи както „пропускането" на заплахи, така и погрешни действия;
- ограничен и контролиран достъп към инженерно-техническите елементи на системата за осигуряване на сигурността на информацията;
- непрекъснатост на работата на СЗИ във всички условия на функционирането на обекта на защита (например при кратковременно спиране на електрозахранването).
- адаптируемост на СЗИ към измененията на средата за сигурност.

Смисълът на повечето от тези принципи е очевиден. Чрез последният се има пред вид, че конфиденциалната информация за способите и средствата за защита на информацията в контингента с времето стават известни на все по- голям брой военнослужещи от контингента, и в резултат се увеличава вероятността на получаването на тази информация от агенти на противника. Затова е целесъобразно периодично да се променя структурата на СЗИ или това да се прави при възникване на реална заплаха от изтичане на информация, например при предателство на военнослужещ, запознат с мерките за сигурност.

При защитата на информация на контингента важна роля играе внедряването на нови научни методи и технически средства. Но и най-съвършените от тях не могат да дадат гаранция за абсолютната защитеност на информацията. Голямо практическо значение има изследването на мотивите, движещи „инсайдерите". Не

е възможно да се подбере абсолютно верен личен състав, а освен това, могат да се допускат и случайни, неумишлени нарушения. Трябва да се осигурява оперативен контрол на поведението и действията на военнослужещите, с цел проверка на тяхната лоялност и установяване на признаци за подготовка и използване на стеганографски продукти срещу сигурността на контингента [18].

Предложените мерки за стеганалогична защита са само началото на конкретни разработки в тази област.

Литература:

1. Семерджиев, Ц. Сигурност и защита на информацията. София: Класика и стил. 2007. ISBN 978-954-327-034-7.

2. Наредба за задължителните общи условия за сигурност на АИС или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация. [онлайн]. [прегледано 20.04.2013]. http://www. dans.bg/ images/ stories/ promzak/naredba_ais_mrezhi-06122012.pdf .

3. Домарев, В. Безопасность информационных технологий. Методология создания систем защиты. Киев: ООО"ТИД"ДС", 2002.

4. Гайкович, В. и Д. Ершов. Основы безопасности информационных технологий. Москва: МИФИ. 1995. [онлайн][прегледан 1 юни 2013].

5. Дворянкин, С. Компьютерные технологии обеспечения безопасности оперативных аудиоданных в условиях информационно-технического противодействия. Дисертация. Москва: 2000.

6. Станев, С, С. Железов. Компютърна и мрежова сигурност. Университетско издателство„Епископ Константин Преславски", Шумен: 2002. ISBN 954-577-306-5. 132 стр.

7. Cox,I., Miller, M., Bloom,J., Fridrich, J. and T. Kalker.Digital Watermarking and Steganography, Second Edition. Elsewier, Morgan Kaufmann Publishers, 2008.

8. Станев, С. Стеганологична защита на информацията. Университетско издателство „Епископ Константин Преславски". Шумен, 2013. ISBN 978-954-577-825-4. 320 стр.

9. Provos, N. and P. Honeyman. Detecting Steganographic Content on the Internet. Univ. Michigan, Ann Arbor, Tech. Rep. CITI 01-la, 2001. [онлайн]. [прегледан 15.05.2012]. http://www.citi.umich.edu/ techreports/reports/citi-tr-01-11.pdf.

10. Conway, M. Code Wars: Steganography, Signals Intelligence, and Terrorism. Knowledge, Technology and Policy (Special issue entitled 'Technology and Terrorism') Vol. 16, No. 2 (Summer 2003): [онлайн]. [прегледан 28.05.2012]. http://doras.dcu.ie/494/1/know_tech_pol_16 _2_ 2003.pdf.

11.US arrest of Russian agents 'reads like spy thriller.The Telegraph, June 29,2010. [онлайн]. [прегледан 30.05.2012]. http://www.telegraph. co.uk/news/worldnews/ northamerica/usa/7860022/US-arrest-of-Russian-agents-reads-like-spy-thriller.html.

12. Ярочкин, В.И. Безопасность информационных систем. Москва: Ось-89, 1996. стр. 208. [онлайн].[прегледан 01юни 2013]. http://www.hist.bsu.by /images /stories/files /uch_materialy /dok/4_kurs /KITDOU _Popova/1.pdf.

13. Steganography and the Insider Threat: Backbone Security Explains Why the IT Security Community Should Take Notice. [онлайн]. [прегледано 20.04.2014]. http://www.sarc-wv.com/news/press_releases/2013/steganography_insider_threat.aspx

14. Simmons, G. The Prisoners' Problem and the Subliminal Channel. Advances in Cryptology: Proceeding in Crypto. CRYPTO'83,1983, pp. 51-67.

15. Асенов, Кипров. Теория на контраразузнаването. София : Труд, 2002.

16. Steganography Analyzer Real-Time Scanner. [онлайн]. [прегледано 20.04.2014]. http://www.sarc-wv.com/products/stegalyzerrts/learn_more.aspx.

17. Землянов, В. Своя контрразведка.Практическое пособие. [онлайн]. [прегледано 20.03.2014].http://coollib.net/b/248996.

18. Христов, Х. Особености на организацията и управлението на оперативното противодействие на посегателства срещу фирмената сигурност. В: Сборник трудове на юбилейна научна конференция „10 години от създаването на НВУ „В.Левски", 2012, Том 4 (под печат).

АНОНИМНА СИСТЕМА ЗА КОМУНИКАЦИИ В КИБЕРПРОСТРАНСТВОТО, ИЗПОЛЗВАЩА ПРОТОКОЛА TOR

Жанета Н. Ташева, Росен А. Богданов

Национален военен университет „Васил Левски"
Факултет „Артилерия. ПВО и КИС", гр. Шумен

ANONYMOUS COMMUNICATION SYSTEM IN CYBERSPACE USING TOR PROTOCOL

Zhaneta N. Tasheva, Rosen A. Bogdanov

ABSTRACT: *Nowadays, the Internet users realize that their surfing in the websites leaves digital fingerprints, which if desired can easily gather and connect to them. Due to this reason, the anonymous communication systems have been developed. Their goal is to enable users to communicate each other anonymously. This paper show how Tor gives users personal freedom, anonymity, privacy and security.*

KEY WORDS: *Anonymity; Anonymous Communication Systems; Tor; Tails.*

ВЪВЕДЕНИЕ

Въпреки своята външна проява, Интернет някога не е бил и не е анонимна среда. При работата си в Интернет потребителите често се държат така, сякаш са анонимни, например публикуват коментари на уебсайтове или сърфират в страници с не толкова легално съдържание в режим на „поверително сърфиране" в браузъра, като смятат, че е невъзможно да бъдат свързани с техните действия. Това не е така, защото при свързване с Интернет, винаги се обявява идентичността на потребителя чрез IP адреса на компютърното устройство, който може да се използва за идентификация или чрез доставчика на интернет услуги, който може да намери чрез сключения договор вашите данни или чрез мрежата фирмата да се идентифицира компютъра по време на работа. Дори при свързване с Интернет от някой IP

адрес чрез свободна WiFi мрежа на хотел, кафе или взето назаем персонално устройство, всеки потребител може да бъде идентифициран от всеки, който наблюдава работата на сесията при влизане в сайтове за социални мрежи или при проверка на уеб-базирана поща .

Все повече потребители вече осъзнават, че използването на Интернет оставя цифрови отпечатъци, които при желание могат лесно да се съберат и да се свържат със съответния потребител [2]. Въпросът за анонимността на потребителите стана още по-наболял след изявлението през юни 2013 г. на директора на програмата PRISM [7], според което Агенцията за национална сигурност NSA (National Security Agency) на САЩ е работила с девет от най-големите доставчици на интернет услуги за масово наблюдение, събиране и съхранение на лични данни след стартиране на програмата през 2007 г. Илюстрация на тези действия е изтичането на информация за личната кореспонденция през 2012 г. на бившия директор на ЦРУ Дейвид Петреъс.

АНОНИМНИ СИСТЕМИ ЗА КОМУНИКАЦИЯ

Според тълковния речник анонимен е обект, който е неподписан, т.е. той е с неизвестен автор или пък авторът е скрит под лъжливо име. Преди появата на компютърните системи и Интернет, поведението като всеки друг субект от обществото е било достатъчно, за да се остане извън полезрението на органите на реда или натрапчивите търговски посредници. Обаче, с появата на компютрите се увеличават и цифровите методи, чрез които потребителите могат да бъдат идентифицирани, като всички те могат да бъдат автоматизирани. Това са IP адрес на устройството, кукитата в използвания браузър и профила на компютърната система, състоящ се браузъра, който използва потребителя, операционната система, инсталираните шрифтове, плъгини и друг софтуер. Това позволява на всеки, който се интересува от даден потребител използващ Интернет, да го следи чрез използването на специален софтуер, който разпознава достъпа и веднага уведомява за него. За решаването на този проблем се използват анонимни системи за комуникация.

Целта на всяка анонимна система за комуникация е да даде възможност на потребителите да комуникират помежду си, като скрива информацията за това кой точно с кого общува. Понятието анонимна комуникационна схеми за първи път е въведено от Chaum [3], който предлага изпращане на съобщения чрез „Смесващ сървър“, който смесва заедно съобщения от няколко податели преди да ги изпрати до техните дестинации, прикривайки реалните взаимовръзки между податели и получатели. Повечето съвременни схеми за анонимност все още практически използват и разширяват тази идея за смесване. Широко използваните съвременни системи за анонимност могат да бъдат категоризирани като системи с висока или ниска латентност [8]. Системите с висока латентност като Mixmaster [10] и Mixminion [5] доставят съобщенията със значително закъснение, средно около 4 часа, с цел да се гарантира анонимност срещу силен противник, който има възможност следи целия мрежов трафик и дори да контрола някои възли, участващи в схемата за анонимност. За да се реализира тази цел, тези системи прилагат контрамерки, като смесване в басейн (pool mixing) и покриване на трафика (cover traffic), която увеличава широчината на използваната честотна лента Смесването в басейн увеличава закъснението, като на всеки рунд се събират редица съобщения, променят се чрез криптиране и поставят в басейна, след което по вероятностен алгоритъм се избират да напуснат басейна.

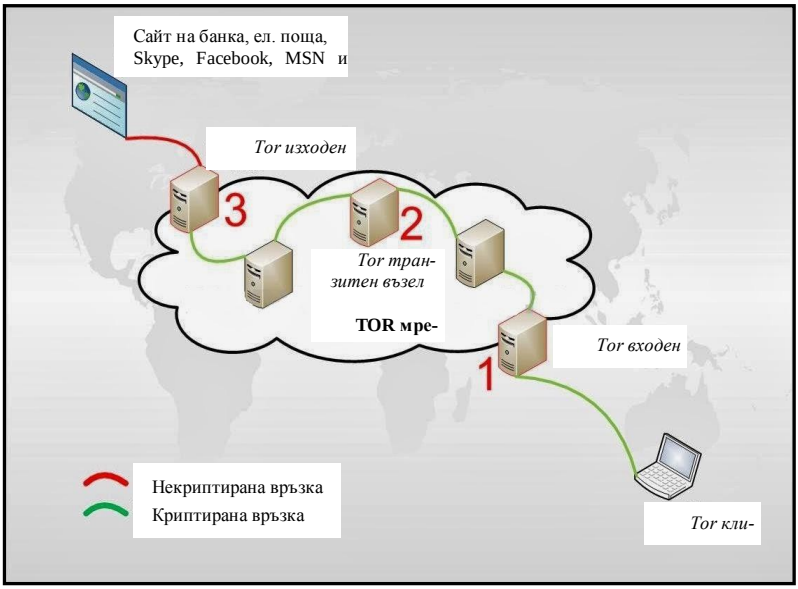
Системите с ниска латентност като Tor [6], I2P [4] и AN.ON [1] се опитват да ограничат закъснението на трафика от допълнителната обработка. Осигуряване на малко закъснение позволява използването за системите за предоставяне на услуги в реално време като дистанционен вход, уеб сърфиране и Интернет чат, но тази функционалност е за сметка на намалени гаранции за анонимност. Тези протоколи са уязвими към активен противник, който може да въвежда в мрежата различни времеви модели на движение на входящия трафик и да търси съответни корелирани модели след излизането му. Съвременните анонимна система за комуникация прилагат средства за осуетяване на тези атаки, но въпреки това повечето реализации защитават предимно срещу анализ на трафика, а не от неговото потвърждаване [8].

Една от най-широко използваните системи за анонимност е система за комуникация използваща протокола Tor. Криптографът Брус Шнаер препоръчва като първа стъпка да се използва системата Tor, за да се осигури защита дори и срещу NSA [12]. Важна предпоставка за използването на Tor е разработката на специална операционна система Tails [13] за работа с протокола. Tails е персонализирана и олекотена Linux дистрибуция, която включва Tor и други функции, за да се предостави ма потребителите операционна система, която подобрява неприкосновеността на личния им живот. Като разработка Tails е подпроект на Tor проекта. В Tails, мрежовият стек е модифициран, така че всяка връзка с Интернет да се пренасочва по подразбиране през Tor мрежата. Ако Tor мрежата не е достъпна, то и публичният Интернет не е достъпен.

АНОНИМНА СИСТЕМА ЗА КОМУНИКАЦИЯ, ИЗПОЛЗВАЩА ПРОТОКОЛА TOR

Различните компоненти, участващи при използването на протокола Tor показани на фиг. 1, са [6], [9]:

- *Tor клиент* (*Tor client*) – софтуер, който работи на компютърна система (PC, нетбук, таблет, телефон и др.), позволяващ свързването с Tor анонимна мрежа. Системата, която използва софтуера на Tor клиент също се нарича Tor клиент.
- *Tor справочна услуга* (*Tor directory service*), състояща се от определен брой сървъри, които поддържат база данни на активните Tor релейни възли и отговаряща на заявките за информация за активни Tor релейни възли.
- *Tor входен възел* (*Tor entry node*) – система, която приема мрежовия трафик от Tor клиенти и го препраща към всеки друг Tor възел. Входният възел може да бъде всякакъв вид Tor релеен възел (изходящ, транзитен или мост). Понеже Tor трафикът е криптиран от Tor клиента към Tor входния възел, е известен само IP адреса на източника (Tor клиента), но не се знае дестинацията и съдържанието на съобщението, което се предава между тях.
- *Tor транзитен възел* (*Tor transit node*) – компютърна система, която приема Tor трафик от Tor възли и го изпраща до други Tor възли. Транзитните Tor възли могат да се използват за създаване на първия или втория скок в Tor веригата. Те не разполагат със средства, с които да се определи дестинацията, за която е предназначен мрежовия трафик и неговото съдържание.
- *Tor изходен възел* (*Tor exit node*) – компютърна система, която може да приеме Tor трафик от всеки друг Tor възел и да го изпрати до желаната публична дестинация в Интернет.



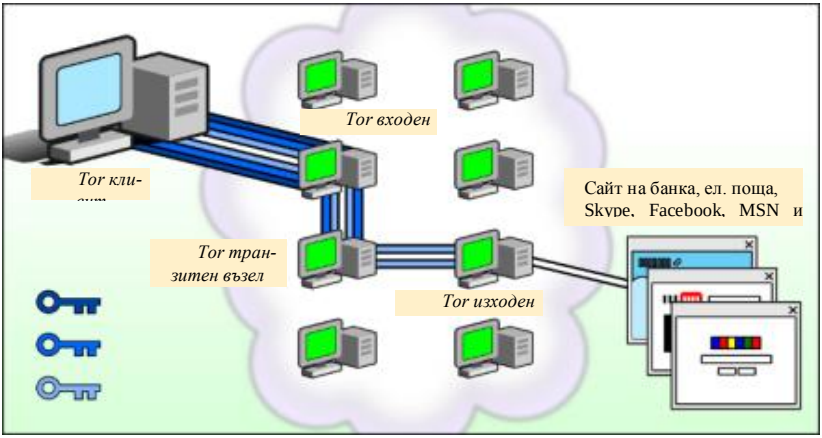
Фиг. 1. *Компоненти на Tor протокола*

Tor клиентът произволно избира маршрут (фиг. 2), състоящ се от един входен, един транзитен и един изходен възел, и след това се договаря веригата за пренос на неговите данни да използва тези възли.

Клиентът криптира данните, които изпраща до местоназначението с помощта на публичния ключ на избрания от него изходен възел (светло синьо на фиг. 2). След това клиентът криптира повторно получените данни с публичния ключ за транзитния възел (синьо на фиг. 2) и накрая, за трети път ги криптира с публичния ключ на входния възел (тъмно синьо на фиг. 2). По този начин Tor клиентът може да изпраща и получава данни в уеб защитен тунел през анонимната Tor мрежа:

- Tor входният възел декриптира пакета със собствения си секретен ключ и го препраща към втория транзитен възел;
- Tor транзитният възел декриптира полученият пакет със собствения си секретен ключ и го препраща към третия изходен възел;
- Tor изходният възел декриптира този пакет със собствения си секретен ключ и го изпраща до местоназначението.

Тъй като входните възли приемат трафик от всеки Tor клиент, противник, който следи даден Tor клиент и установи начало на Tor верига, знае със сигурност само, че този клиент използва Tor и избрания Tor входен възел. Входният възел ще предаде трафика на клиента, както и трафика на други клиенти, до други Tor транзитни възли. Противникът няма да бъде в състояние да разбере точно кой трафик към кой транзитен възел отива, тъй като има достатъчно други Tor потребители, използващи същия входен възел.



Фиг. 2. *Изграждане на сигурен тунел чрез публичните ключове на Tor възлите*

Вторият скок от транзитния възел препраща трафика към изходния възел без да знае за трафика, който е изпратен от Tor клиента. Тъй като данните се предават и в двете посоки чрез Tor мрежата, криптираните слоеве са „неразопаковани“ като лук, откъдето произлиза и наименованието „Лук маршрутизиране“ (onion routing).

По този начин, с местоназначението може да бъде свързан само Tor изходният възел. Вътрешният транзитен възел може да бъде свързан само с входни и изходни възли, в резултат на което комуникационната верига ефективно изтрива връзката между Tor клиента и Интернет сървъра, с който той се свързва.

Целият мрежов трафик излизащ от Tor мрежата изглежда така, сякаш той влиза в Интернет от Tor изходните възли, а не от оригиналните клиентски възли. Ето защо цялата Tor мрежа функционира като едно прокси: всички данни постъпили в него многократно се криптират и препакетират, с цел да се направи така, че сякаш всичко идва от възела изход. По същия начин, целият входящ трафик изглежда, че идва от избрания от клиента входен възел, вместо от действителния, може би блокиран, сървър.

Това е способност, която прави Tor полезен в случаите, когато национални защитни стени блокират целия трафик към някои сайтове. По същата причина, потребителите на Tor могат да сърфират в Интернет, без да предоставят своя IP адрес, който може почти винаги да бъде свързан директно с конкретно местоположение.

ПРИЛОЖЕНИЕ И СИГУРНОСТ НА АНОНИМНАТА СИСТЕМА ЗА КОМУНИКАЦИЯ TOR

Tor позволява на потребителите да получат достъп и дори да публикуват съдържание в Интернет, без да се налага то да бъде съобразено с изискванията на органите на властта, по начин позволяващ да се избегне тяхното откриване и идентифициране. Разбира се, риск от „погрешни“ действия чрез Tor съществува. Възможен е достъп на дете до уеб сайтове, забранени от родителите му, достъп на служител до сайтове, забранени от ръководството на фирмата, или достъп на гражданин до уебсайтове, забранени от правителството. Затова някои хора гледат на Tor

като заплаха, която ще позволи на престъпниците да извършват престъпления безнаказано. Проблемът с този аргумент е, че всеки, който е решил да извърши престъпление с Tor, може да реализира целта за анонимност чрез други престъпни методи, като откраднe телефон или компютър и се свърже към ботнет мрежа за управление на тези устройства. Хората, които развиват и подкрепят Tor го правят, защото те силно вярват в правата на човека и необходимостта от анонимност, за да се защитят тези права, особено в ситуации, в които упражняването на тези права без анонимност ще донесе вреда.

Tor първоначално е бил разработен с финансиране от Американската лаборатория за военноморски научни изследвания (US Naval Research Laboratory) с намерението Tor да се използва за защита на правителствените комуникации. Съществуват множество военни приложения на Tor [9]:

- При операции под прикритие и полеви такива може да се използва Tor, за да се избегне откриването им от противници, способни да извършват мониторинг на мрежовата активност. Tor предоставя средство за тайно свързване към системи, за които се знае, че са под контрола на военните (IP адреса на регистрация е публичен, включително IP адресите на правителства и военни).
- Специални скрити услуги могат да се използват за събиране и разпространяване на информация за командни и контролни функции, без да се разкриват местонахождението на услугата и мястото/самоличността на тези, които използват тези услуги.
- Събиране на разузнавателна информация, по-специално чрез свързване към ресурси, използвани от противника (уеб сървъри, онлайн форуми и др.), без предоставяне на истинското местоположение на организацията, което може лесно да се определи от IP адреса и мрежовия клиент.

Журналисти, включително блогъри и други граждански организации, използват Tor, за да защитят себе си докато предават от части на света, където има небезопасен достъп до Интернет, както и за защита на техните източници, които желаят да останат анонимни.

Служители и агенции на законодателни органи могат да използват Tor за разследвания и операции, като:

- Събиране на информация от съмнителни сайтове или мрежови услуги, използвани за незаконни дейности.
- Стартиране на операции под прикритие, без да се разкрива, че системите използват IP адреси, регистрирани на правоприлагащи агенции.
- Анонимна помощ, свързана с правата на човека и срещу корупцията, отправяна към правоприлагащи агенции без да разкрива идентичността на източника.

Tor може да бъде полезна мрежа за всеки, който участва активно в публичната сфера, при опити да намери начин да изрази своите непопулярни мнения по въпроси, които да не бъдат свързани със съответната обществена личност.

По същия начин, Tor може да е полезен и за обикновените хора, които искат да изразят своите становища или изследователски въпроси, които могат да бъдат погрешно изтълкувани или да предизвикат нежелано внимание. Чрез Tor, всеки може да изрази своите становища, без страх от възмездие или дискриминация от страна на работодателите или други органи за излагането на своето мнение.

Бизнесмени и специалисти в областта на информационните технологии (ИТ) използват Tor като важен инструмент за редица цели, включително:

- Достъп до онлайн ресурси анонимно, особено когато те използват филтри, за да цензурират информацията, която се предоставя на потребители, които сърфират в интернет страниците им от техните мрежи на конкурентите.
- Осигуряване на възможност за анонимност на служители, които желаят да представят отрицателна информация на ръководството.
- ИТ специалистите могат да използват Tor за оперативно тестване сигурността на корпоративните защитни стени и другите мрежови ресурси без да се правят каквито и да било промени в защитната стена.

След последните експертни анализи и съобщения в средата на 2013 г. NSA могат да разбиват 1024 битовите RSA/DH (Rivest, Shamir and Adleman/Diffie–Hellman) ключове. Проблемът с Tor [11] е, че той все още използва тези 1024 битови ключове в криптографските алгоритми, тъй като по-голяма част Tor потребителите (около 76%) използват по-старата версия 2.3 на Tor софтуера. По-новата версия 2.4 е подобрена, като тя позволява да се прилагат ключове с по-голяма дължина, но само 24 % от Tor потребителите я използват. Въпреки съобщенията за този недостатък, Tor и операционната система Tails предлагат на потребителите възможност за достъп до блокирани сайтове и сърфиране в Интернет без да предоставят своя IP адрес.

ЗАКЛЮЧЕНИЕ

Полезността на Tor мрежата при предоставяне на услугата анонимност е в това, че няма начин всички Tor потребители да се категоризират от една страна като „престъпници“ или от друга като „правителствени органи“. Tor потребителят може да бъде престъпник, но също така той може да бъде жертва на престъпление или полицай под прикритие, дипломат, политически активист или обикновен гражданин. Именно, наличието на разнообразни потребители в Tor мрежата я прави полезна, защото по този начин тя позволява на всеки да скрие по-успешно своята самоличност.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. Anonymity.Online: Mixes for Privacy and Anonymity in the Internet Documentation. Project Anonymity in the Internet. Germany. 2013. Available at http://anon.inf.tu-dresden.de/develop/doc/mix_short/.
2. Boyanov, P. K. „A taxonomy of the cyber attacks.“ *Journal Scientific and Applied Research*, Vol. 3, 2013, pp. 114-124.
3. Chaum, D. L. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM* Vol. 24, No. 2, 1981. pp. 84-88.
4. Cox, J. I2P - Anonymity for the Masses, November 11, 2011.
5. Danezis, G., Dingledine, R., and Mathewson, N. Mixminion: Design of a Type III Anonymous Remailer Protocol. *In Security and Privacy 2003. Proceedings 2003 IEEE Symposium on Security and Privacy (Washington, DC, USA, 2003), IEEE Computer Society*, pp. 2-15.
6. Dingledine, R., Mathewson N., and Syverson P. *Tor: The Second-Generation Onion Router*. Naval Research Lab Washington DC, 2004.
7. Director of National Intelligence. Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Washington, DC 20511, June 8, 2013. Available at:

http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf.

8. Hopper, N., Vasserman, E. Y., and Chan-Tin, E. How much anonymity does network latency leak?. *ACM Transactions on Information and System Security (TISSEC)*, Vol. 13. No. 2, 2010, pp. 1322.

9. Loshin, P. *Practical Anonymity: Hiding in Plain Sight Online*. Elsevier Inc. 2013. ps. 131. ISBN: 978-0-12-410404-4.

10. Moeller, U., Cottrell, L., Palfrader, P., and Sassaman, L. Network Working Group Internet-Draft: Mixmaster protocol version 2. 2005. Available at: http://tools.ietf.org/pdf/draft-sassaman-mixmaster-03.pdf.

11. Owano, N. Next question: can the NSA crack Tor keys? September 09, 2013. Available at: http://phys.org/news/2013-09-nsa-tor-keys.html.

12. Schneier, Br. How to Remain Secure Against the NSA. September 2013. Available at: https://www.schneier.com/blog/archives/2013/09/how_to_remain_s.html.

13. Tails. The amnesic Incognito Life System: Documentation. Available at: https://tails.boum.org/doc/index.en.html.

КОНЦЕПТУАЛНИ АСПЕКТИ НА КИБЕРСИГУРНОСТТА

Галин Р. Иванов

Военна академия „Георги Стойков Раковски“, Катедра „Мениджмънт на сигурността и отбраната“, България, София, п.к. 1504, бул. „Евлоги и Христо Георгиеви“ № 82, тел:+359 2 92 26670, Факс: +359 2 92 26544, iwanow_off@abv.bg

CONCEPTUAL ASPECTS OF CYBERSECURITY

Galin R. Ivanov

ABSTRACT: *The increase in outbreaks in the information which led to the need for systematic analysis of the sources of threats. Requires harmonized between trained professionals and operational concept in the field of cybersecurity.*

KEY WORDS: *information security, cybersecurity, cyberspace , cybercrime.*

В момента се наблюдава рязко увеличение на инциденти в областта на киберинформационната сигурност, които са широко разпространени и придобиват заплашителни размери. Много подобни атаки засягат широк кръг от частния и корпоративния бизнес и правителствените интереси. Инцидентите в областта на киберсигурността стават все по-чести, по-значителни и по-комплексни и за тях няма граници. Тези инциденти могат да причинят значителни щети на безопасността и на икономиката на дадена държава.

Съдържанието на термина „Киберсигурност“ се основава на думата „Кибернетика“ (от гръцки „изкуство на управление“) - Наука за законите на получаване,

съхраняване и предаване на информацията, както и за системните носители на изкуствен интелект [4]. Абстрактната кибернетична система представлява съвкупност от предварително взаимосвързани помежду си по обем обекти, наречени елементи на системата, способни да възприемат, съхраняват и обработват информация, както и да обменят такава.

Към предметната област на кибернетиката и киберсигурността се включват всички съвременни информационни и телекомуникационни технологии. Важно е да се отбележи, че елементите на киберсигурността в рамките на кибернетичния подход се третират като непрекъснато взаимодействие между себе си и действат в качеството си на важни съставни елементи в киберпространството и включват:

- Информацията в реално време.
- Хората, които са активни участници в областта на информационния обмен и използване на информационните ресурси.
- Софтуера и хардуера.
- Глобалната информационна среда.

Какви са доказаните факти за киберсигурността днес?

- Киберпрестъпността причинява не малък дял от инцидентите в киберпространство.
- Според Световния икономически форум има 10-процентна вероятност от значителен срив на критична информационна инфраструктура през следващото десетилетие, което би могло да нанесе щети от 250 млрд. щатски долара.
- Всеки ден циркулират около 150 000 компютърни вируса и 148 000 компютъра биват компрометирани.
- Според изследване на Symantec жертвите на киберпрестъпленията в световен мащаб губят около 290 млрд. EUR всяка година. Друго проучване на McAfee показва, че приходите за киберпрестъпността са 750 млрд. евро годишно.
- Анкетата на Евробарометър за киберсигурността за 2012 г. установи, че 38 % от потребителите на интернет в ЕС са променили поведението си от съображения за киберсигурност: за 18 % има по-малка вероятност да закупуват стоки онлайн и за 15 % е по-малко вероятно да използват онлайн банкиране. Анкетата също така показва, че 74 % от анкетираните са съгласни, че рискът да станат жертва се е повишил, 12 % вече са били жертва на онлайн измама и 89 % избягват разкриването на лична информация [5].
- От данните на Евростат е видно, че от януари 2012 г. само 26 % от предприятията в ЕС са имали официално определена политика за защита на информационни и комуникационни технологии [6].

Основните аспекти на киберзаплахата днес са, както следва:

- Увеличаване на броя на атаки, много от които водят до големи загуби.
- Увеличаване на ръста и сложността на кибератаките, които могат да включва няколко етапа и се прилагат специални методи на защита срещу възможни методи на противодействие.
- Въздействие върху почти всички електронни (цифрови) устройства, включително и всички мобилни устройства.
- Все по-честите нападения върху информационната инфраструктура на големите корпорации, на важните промишлени обекти, критична инфраструктура и дори държавни агенции и министерства.

➢ Използването на най-напредналите в областта накомпютърни технологии страни, чрез интелектуалните си ресурси и новите методи за кибератаки да извършват кибернападения срещу други държави.

Това се потвърждава и почти всеки ден в електронни бюлетини и новини, които изобилстват от информация за нови атаки от престъпници в информационната сфера.

Изявленията на бившият шпионин на ЦРУ Едуард Сноудън потвърждават активното участие на държавните структури на развитите страни в областта на киберсигурността за добиване и събиране на информация за граждани, длъжностни лица, високопоставени политически лидери, корпорации и друга на пръв поглед публично достъпна информация, която може да бъде агрегирана за да се постигне кумулативен ефект за получаване на конфеденциална информация. С цел да се манипулира обществеото мнение, чрез организирани и предварително подготвени групи от хора целенасочено и активно се прилагат специални методи за социално инженерство чрез средствата за комуникация през интернет. Ефектен пример за това е продължаващата криза в Украйна. По този начин, има редица проблеми в областта киберсигурността, които не могат да бъдат напълно решени от традиционните средства и на които трябва да се обърне внимание на нашето обществото и държавните власти.

Мащабните нарушения на киберсигурността, които засягат всички области на обществения живот в страната, в основата на които лежат методите за осъществяване на кибератаки на компютърни мрежи, а също така и въздействие и индиректно управление на публично съзнание на хората изисква систематичен подход към интегрирана система за сигурност, способна да противодействие на тези заплахи.

В последните 5-6 години се появиха изключително сложни елементи на кибератака, насочени към влошаването на промишлени обекти и критична инфраструктура. През 2009 г. е установено, че действа червея Stuxnet, а през тази година са разработени червеите Duqu и Flame, последния от които е с много сложна архитектура. В информационното пространство се прокрадна информация за участието на експерти на американското разузнаване, които са създатели на тези сложни зловредени софтуери и съпричастността на правителствени структури, които оказват финансова подкрепа за атаки в киберпространството[7].

Документирани са многобройни кибератаки срещу най-големите банки в САЩ. Тези атаки биха могли да унищожат напредналите системи за защита и да осъществят реална заплаха за националната инфраструктура. Експерти в областта на киберсигурността предполагат, че тези атаки вероятно са организирани от Китай [8].

В края на 2012 г., държавните структури на САЩ и Китай публично изразиха своите подозрения за създаване оборудване с недокументирани възможности, чрез които една държава атакува мрежа на друга страна. Под съмнение са продуктите на компании Huawei и ZTE от китайска страна и компанията Cisco от американската страна [9].

През 2013 г., Лабораторията на Касперски публикува информация за чисто ново явление в компютърните атаки. Била е разкрита шпионска мрежа наречена „Червения октомври“, която в продължение на пет години е била ангажирана в кражба на държавни тайни. Този сложен комплекс от злонамерен софтуер, с около1000 злонамерени файлове, свързани с 30 различни групи модули [10]. Аналогичен метод вече активно се използва и за мобилните устройства, работещи с Android [11].

В стандарта (ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity) свързан с Информационни технологии –Техники на сигурност - Насоки за киберсигурността) **киберпространството** е дефинирано като сложна среда, несъществуваща в някаква физическа форма, възникваща в резултат от взаимодействието на хора, софтуер, интернет услуги чрез технически устройства и мрежови връзки.

В програмна статия за киберсигурността на експерти от Великобритания, определят понятието „**киберпространство** *като всяка дейност в мрежата изразена чрез цифрово изражение, което включва също и съдържанието на информацията и действия извършвани посредством цифровите мрежи“[12].*

Основното съдържание на киберпространството се заключава в активността на потребителя на цифрово съдържание и инфраструктура от информационно-комукационни технологии.

Киберпространството може да се разглежда като триада, която включва три основни компонента:

- **Информация в своето цифрово изображение:**

-статични (файлове, записани на носителиданни);

-динамични (пакети, потоци, команди, искания и др., предавани по различни мрежи, преработени в автоматизирани системи и инструменти, представени за показване в графичен или табличен формат).

- **Техническа инфраструктура, информационно-комукационни технологии, софтуер,** с помощта на които се осъществяват основните действия свързани с информацията: събирането обработването, съхранението и предаването й. Тези инструменти включват инфраструктурата на интернет и мрежови връзки, компютри и др.
- **Информация между субектите** сизползване на информацията, получена (предавана) и обработена от техническата инфраструктура. Това се отнася до всички дейности на потребителите в киберпространството. Потребителите се стремят към целенасочено използване на информационни ресурси, потоци и складове, които се намират на техническа инфраструктура.

Съвкупността от тези три компоненти взети заедно образуват единен компонент, който може да се нарече киберпространство.

От особена важност е да се формулира понятието киберсигурност и да се определят основните цели за защита на киберпространството и възможните възникващи заплахи. Киберсигурността не може да бъде насочена за защита на максималния брой на заплахи. Необходимо е да бъде гарантирана най-благоприятната среда за всички потребители и системи в киберпространството.

Киберсигурността, *както и киберпространството може да се опише с триадата на нейните съставни компоненти, определени в композитна част на киберпространството, а именно съвкупност от условия, при които информационни ресурси, компютърни и мрежови архитектури (инфраструктура) и начини на взаимодействие между потребителите са защитени от максимално число заплахи и въздействия с нежалателни последствия.*

Киберсигурността *обхваща не само информацията за защита като обект за защита, но и технически средства чрез които се определя как да цирку-*

лира информацията между потребителите, начините и средствата за защита в киберпространството.

За в бъдеще е необходимо подробно и внимателно да се изследват основните свойства на киберпространството, динамиката на своето развитие в различни мащаби и да се разработят многовариантни процедури за управление на тази динамика. Без систематичен анализ и получаване на реална оценка на прилагането на мерките за безопастнот е невъзможно да се изгради ефективна система за киберсигурност.

И в заключение трябва да отбележа, че е нужно да бъдат предприети следните мерки в краткосрочен и дългосрочен план за подобряване на киберсигурността на национално ниво:

1. Създаване на единен държавен мониторингов ситуационен център за контрол и защита на киберпространството, информацията и телекомуникационна инфраструктура и междуведомствени ситуационни специализирани центрове за противодействие на кибертероризма и кибератаки.

2. Подобряване на системата за подготовка на кадри включваща обучението и квалификация в сферата на киберсигурността.

Използвана литература:

1. Антонович П.И., О современном понимании термина „кибервойна“, Вестник Академии военных наук. № 2 (35), 2011.

2. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросыкибербезопасности., № 1 (1), 2013.

3. Макаренко С. И., Информационная безопасность: учебное пособие для студентов вузов, Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009.

4. Български тълковен речник, Издателство „Наука и изкуство”, София, 1994.

5. http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf (17.00 часа 16.05.2014).

6. http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises (15.03 часа 22.05.2014).

7. http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report/cyber-attacks.aspx (14.23 часа 24.05.2014).

8. http://www.cybersecurity.ru/crypto/171331.html (17.10 часа 24.05.2014).

9. http://www.cybersecurity.ru/telecommunication/165487.html (10.10 часа 27.05.2014).

10. http://habrahabr.ru/company/kaspersky/blog/169839/ (12.10 часа 29.05.2014).

11. http://www.itsec.ru/newstext.php?news_id=91005 (15.33 часа 27.05.2014).

12. Klimburg A. etal. National cybersecurityframeworkmanual //NATO CCD COE Publications(December 2012).–http://belfercenter.hks.harvard.edu/files/hathaway-klimburg-nato-manualch-1.pdf) (16.42 часа 30.05.2014).

ПРИЛОЖЕНИЕ НА FPGA ЗА ИЗГРАЖДАНЕ НА УСТРОЙСТВА ЗА КРИПТИРАНЕ НА ДАННИ

Милена Х. Ламбева

Национален военен университет „Васил Левски”,
Факултет „Артилерия. ПВО и КИС”, гр. Шумен

FPGA-based implementation of the encryption/decryption devices

Milena H. Lambeva

ABSTRACT: *Subject of this work is the architecture of FPGA, the implementation of encryption / decryption devices on such chips and use of intellectual cores to accelerate the design process.*

KEY WORDS*: data encryption, FPGA, IP core.*

Повишаването на значимостта на информацията в качеството й на ресурс, и увеличаването обмена на данни във всяка сфера на обществения живот доведе до нарастването на необходимостта от гарантиране на нейната сигурност при предаване и съхраняване.

Много стар подход за обезпечаване на поверителността на информацията е подлагането й на криптографско преобразуване. *Криптирането* се изразява в трансформиране на данните преди предаването им по комуникационния канал, посредством определен математически метод – *алгоритъм за криптиране/декриптиране*, с използване на секретна информация – *криптографски ключ*. Трансформацията, която се извършва при получателя, с цел възстановяване на първоначалната информация се нарича декриптиране.

Когато двете страни използват един и същ, предварително придобит ключ криптирането се нарича симетрично. Американският Национален институт за стандарти и технологии *(**N**ational **I**nstitute of **S**tandards and **T**echnology)*[8] е утвърдил следните *симетрични алгоритми: Data Encryption Standard (DES), Triple Data Encryption Algorithm (3DES), International Data Encryption Algorithm (IDEA)* и *Advanced Encryption Standard (AES*) и др., и редица *асиметрични - RSA, Diffie-Hellman* и *Elgamal,* които прилагат уникална двойка ключове - публичен и частен, за шифриране и дешифриране.

Разнообразието от алгоритми е отговор на усъвършенстването на средствата за компрометиране на данни, и на все по–осезаемата необходимост от бързодействие и сигурност при предаването и съхраняването им.

Изпълнението на софтуера, реализащ тези сложни математически преобразувания, следва да се от хардуерна платформа с високо бързодействие, надеждност на работата, ниска цена и малки размери. За апаратна реализация на криптира-

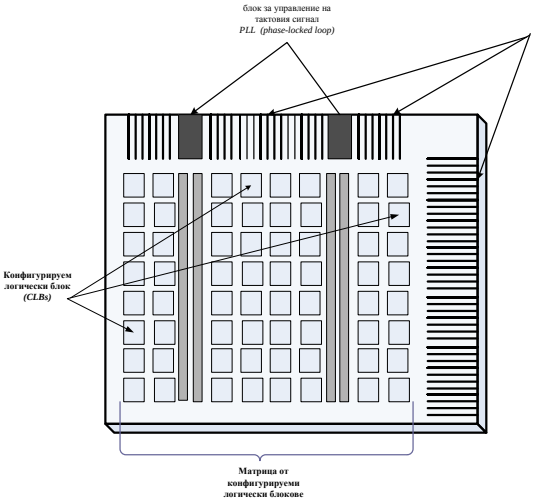
щи/декриптиращи устройства с такива характеристики все по-често се използват програмируемите логически матрици *(field-programmable gate array).*

Логическа матрица с програмируеми полета е интегрална схема, изградена от голям брой конфигурируеми по електрически път логически блокове, и ресурси за осъществяване на връзки между тях. Отличава се с голяма гъвкавост при реализация на проекти поради възможността за многократно конфигуриране на чипа. Програмирането се реализира както на всеки логически и функционален блок за изпълнение на различна логическа или аритметическа функция, така и на съединенията между блоковете, за целта се използват познатите езици за хардуерно описание – Verilog или VHDL, в съчетание с традиционно осигурени от производителя на чипове интегрирани развойни среди Quartus (Altera Corporation), ISE® Design (Xilinx).

Обобщената архитектура на произволен FPGA чип включва следните пет основни програмируеми функционални елемента:

- Програмируеми логически блокове за реализация на логически и аритметични функции и за съхраняване на данни.
- Входно/изходни блокове за контролиране на предаването на данни между входно/изходните изводи и вътрешната логика на чипа.
- Блокове RAM.
- Блокове за умножение.
- Блокове за управление на тактовия сигнал.

Примерното им разположение върху произволен чип е представено на фигура 1.



фиг. 1. Блокова диаграма на произволна FPGA

Програмируемите логически блокове (***C**onfigurable **L**ogical **B**loc – **CLB**),* от порядъка на десетки или стотици хиляди са подредени са в двумерна матрица, наречена логически масив (*logic array*). Те изпълняват логически, аритметични функ-

ции, запомнящи функции и функции по формиране на входно/изходните сигнали за чиповете. Връзката между тях се осъществява посредством линиите и буферните схеми на конфигурируема комуникационна матрица. Елементите на архитектурата на програмирумия блок са:

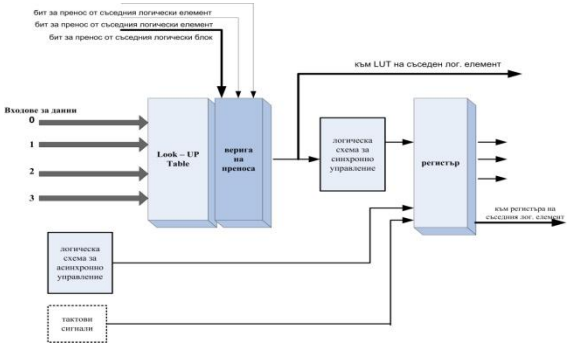
- Определен брой (4, 6 или 10) *елементарни логически елементи*
- логически вериги за управление на преноса;
- логика за формиране на контролни сигнали;
- логически вериги между запомнящите елементи;
- логически вериги между функционалните таблици;
- локален интерфейс (между логическите елементи на блока);

Елементарните логически елементи са най–малките функционални единици, предназначени за изпълнение на дефинираните от потребителя логически функции. Практически те се реализират от n-входова комбинационно – логическа схема, наречена функционална таблица ***(Look-Up Table** – LUT*). Тя формира коя да е от възможните $F = 2^{2^n}$ функции от ***n*** променливи и я запомня в регистър.

Елементарния логически елемент има в архитектурата си още: логическа верига на преноса и интерфейси: вътрешен (между компонентите на елемента), за връзка със съдените в реда и колоната елементи на същия логически блок.

Броят на програмируемите логически блокове в чипа на различните устройства от фамилията *Altera® Cyclone* варира от 2 910 до 20,060. Всеки логически блок е изграден от 10 логически елемента, чиято архитектура е представена на фигура 2. Основните и функционални блокове са:

- една LUT за реализация на произволна, потребителски дефинирана логическа функция от четири променливи;
- един програмируем регистър;
- логическа верига за управление на запомнящия елемент;
- логическа верига на запомнящия елемент връзка с регистрите на съседните логически елементи;
- логическа верига на функционалната таблица;



Фиг. 2. Обобщена блокова схема на логически елемент на *Altera® Cyclone*.

Елементарният логически елемент притежава четири линии за входни данни, от където постъпват стойности на променливите за LUT, логиката за управление на

преноса има трибитов вход (един бит за отчитане на преноса от съседния логически блок и два бита за пренос от съседния логически елемент). Запомнящият елемент може да бъде програмиран за работа в режим на D, T, JK, или SR тригер, притежава входове за синхронно и асинхронно въвеждане на данни и три битов изход, които са изходи и на самия логически елемент.

Архитектурата на логическите елементи, на логическите блокове и на програмируемите прибори на различните производители варира в зависимост от заложените характеристиките и цена. Наблюдава се тенденцията за увеличаване на капацитета и функционалността, чрез увеличаване на броя на логическите елементи и вграждане на памети и други функционални блокове, и намаляване на цената.

Табл. 1. Характеристики на Stratix V GX

Характеристика	5SGXA3	5SGXA4	5SGXA5	5SGXA7	5SGXA9	5SGXAB	5SGXB5	5SGXB6
Брой Логически елементи	340	420	490	622	840	952	490	597
Брой регистри	513	634	740	939	1,268	1,437	740	902
M20K Memory Blocks	957	1,900	2,304	2,560	2,640	2,640	2,100	2,660
Брой мултиплексори	512	512	512	512	704	704	798	798

Допълнително предимство е възможността за повторно използване на инженерния труд (*design reuse)* под формата на свободно разпространявани или платени интелектуални ядра ***(Intellectual Property core***). Тази практика има за цел облекчаване на проектантския труд и скъсяване на времето за разработка на изделието.

Интелектуалните ядра са готови функционални блокове от предварително проектиран, създаден и тестван софтуер, разпространяван най-често под формата на VHDL или Veriolg RTL програмен код, който може да се тества и модифицира от потребителя преди да бъде вграден в чипа – софт ядро, или е предварително вградени в чип – хардуерно ядро.

Съществува разнообразие от платени или свободни за ползване IP-ядра. Производителите на FPGA чипове предлагат в техните CAD системи библиотеки, съставени от набор IP-ядра, при това технологично съобразени с конкретно използваната логика – *Xilinx CoreGenerator [9], Altera MegaCore IP[5]* например.

В таблица 2 е представена малка част от списъка с IP ядра за симетрично криптиране и хеширане, разпространявани от Altera® и нейни партньори, оптимизирани за съответните устройства.

Очевидна е съвместимостта на всяко от IP ядрата с няколко фамилии fpga матрици. Пример за това е единия от предлаганите от CAST, Inc. [6] модули - AES Codec (AES C), за криптиране и декриптиране на данни с алгоритъм на Рейндал.

Таблица 2. Интелектуални ядра за криптиращи алгоритми

Наименование на продукта	Съвместимост	Доставчик
High-Speed AES Encryption/Decryption Cores	Stratix III E, Cyclone III, Stratix II GX, Arria GX, Cyclone II	D'Crypt Pte. Ltd.
AES Codec (AES C)	Cyclone IV GX, Cyclone III LS, Stratix IV GX, Arria II GX, Stratix III E, Cyclone III, Stratix II GX, Cyclone II, Stratix II, Stratix	CAST, Inc.
AES Programmable Codec (AES P)	Cyclone IV GX, Cyclone III LS, Stratix IV GX, Arria II GX, Stratix III E, Cyclone III, Stratix II GX, Cyclone II, Stratix II, Stratix	CAST, Inc.
AES Encryption / Decryption cores	Cyclone V GX, Cyclone V GT, Arria V GX, Arria V GT, Arria V GZ, Stratix V GX, Stratix V GT, Arria II GX, Arria II GZ, Stratix IV GX, Stratix IV GT	intoPIX
Multi-Purpose AES Crypto Engine (BA411E)	S tratix III L, Stratix III E, EP4E, Stratix IV GX, Stratix IV GT, Stratix V E, Stratix V GS, Stratix V GX, Stratix V GT, Cyclone III LS, Cyclone IV E, Cyclone IV GX, Arria II GX, Arria II GZ	Barco Silex
Triple DES Encryption	Cyclone IV GX, Cyclone III LS, Stratix IV GX, Arria II GX, Stratix III E, Cyclone III, Stratix II GX, Cyclone II, Stratix II, Stratix	CAST, Inc
DES/3DES Encoder / Decoder (BA412)	Stratix III L, Stratix III E, EP4E, Stratix IV GX, Stratix IV GT, Stratix V E, Stratix V GS, Stratix V GX, Stratix V GT, Cyclone III LS, Cyclone IV E, Cyclone IV GX, Arria II GX, Arria II GZ	Barco Silex
RSA Public Key Accelerator Core	Cyclone V GX, Cyclone V GT, Arria V GX, Arria V GT, Arria V GZ, Stratix V GX, Stratix V GT, Arria II GX, Arria II GZ, Stratix IV GX, Stratix IV GT	intoPIX
Public Key Crypto Engine (BA414E)	Stratix III L, Stratix III E, EP4E, Stratix IV GX, Stratix IV GT, Stratix V E, Stratix V GS, Stratix V GX, Stratix V GT, Cyclone III LS, Cyclone IV E, Cyclone IV GX, Arria II GX, Arria II GZ	Barco Silex
Hashing IP Core (BA413)	Stratix III L, Stratix III E, EP4E, Stratix IV GX, Stratix IV GT, Stratix V E, Stratix V GS, Stratix V GX, Stratix V GT, Cyclone III LS, Cyclone IV E, Cyclone IV GX, Arria II GX, Arria II GZ	Barco Silex
SHA-1 (Secure Hash Algorithm) Processor	Cyclone IV GX, Cyclone III LS, Stratix IV GX, Arria II GX, Stratix III E, Cyclone III, Stratix II GX, Cyclone II, Stratix II, Stratix	CAST, Inc.
SHA-256 (Secure Hash Algorithm) Processor	Cyclone IV GX, Cyclone III LS, Stratix IV GX, Arria II GX, Stratix III E, Cyclone III, Stratix II GX, Cyclone II, Stratix II, Stratix	CAST, Inc.

Както е показано в таблицата, кода може да бъде вграден в много представители на фамилиите Cyclone и Stratix на Altera®. Ядрото има осигурява прилагане на 128, 192 и 256 – битов ключ, както и динамична промяна на режима на работа (криптиране или декриптиране). Предлага се в две архитектурни версии:

- *Стандартна версия (**AES32-C**)* – обработва 32 – битов поток от данни, за 44/52/60 такта с използване съответно на 128, 192 и 256 – битов ключ;
- *Ускорена версия (**AES128-C**)* - обработва 128 – битов поток от данни, за 11/13/15 такта с използване съответните ключове, достига скорост от 2 Gbps.

Ядрото е преминало верификация съгласно стандарта AES FIPS 197[8]. Подходящо е за вграждане в редица устройства: защитени мрежови рутери, устройства за безжична комуникация и криптиране на данни. Изпълнява стандартните AES – преобразувания в следните стандартни режими:

- режим електронна кодова книга (ECB — Electronic Code Book),
- режим свързване на блокове (CBC — Cipher Block Chaining),
- режим обратна връзка по шифротекст (CFB — Cipher Feed Back),
- режим обратна връзка по изход (OFB — Output Feed Back).

В таблица 3 са показани данни за реализацията на ядро *AES32-C* върху различни платформи (брой на използваните: логически елементи, I/Os и RAM) и максималната тактова честота и скорост на обработка на данните.

Табл. 3

Фамилия	***Брой логически елементи***	***RAM***	***I/Os***	***F max (MHz)***	***Скорост MBps***	***Версия на Quartus***
Cyclone EP1C12 -6	792	10 M4K	115	111	321	7.2
Cyclone - II EP2C20 -6	779	10 M4K	115	119	345	7.2
Cyclone - III EP3C120 -6	789	6 M9K	115	136	394	7.2
Stratix EP1S10-5	760	10 M4K	115	113	327	7.2
Stratix - II EP2S15-3	632	10 M4K	115	192	556	7.2
Stratix - III EP3SE50-2	630	6 M9K	115	208	603	7.2

** данните в таблицата са резултат от експеримент, проведен от CAST, Inc. и са публикувани на адрес: http://www.cast-inc.com/ip-cores/encryption/aes-c/cast_aes-c-a.pdf*

Проектирането на устройства за криптиране и декриптиране на базата на програмируеми схеми се характеризира с голяма гъвкавост и универсалност. С веднъж проектирано функционалното описание, реализацията на устройството се свежда до програмирането на интегралните схеми, което също става направо в крайното устройство.

FPGA са подходящи за хардуерна реализация на ефективни устройства, силно ограничени по отношение на размери и цена.

Литература:

1. FX. Standaert, G. Rouvoy, JJ. Quisquater, JD. Legat. A Methodology to Implement Block Ciphers in Recon_gurable Hardware and its Application to Fast and Compact AES Rijndael. In the proceedings of FPGA 2003, pp. 216-224, ACM
2. Gonzalez I., Lopez – Buedo S., Gomez F., Martinez J., Using Partial Reconfiguration in Cryptographic Applications: An Implementation of the IDEA Algorithm, сборник доклади 13 – та международна конференция Field-Programmable Logic and Applications, Lisabon Септември 2003 г
3. Rouvroy G., Standaert FX.., Quisquater JJ., Legat JD., Compact and Effcient Encryption/Decryption Module for FPGA Implementation of the AES Rijndael VeryWell Suited for Small Embedded Applications, ITCC 2004 (Las Vegas, USA, April 2004)., на адрес: http://hdl.handle.net/2078.1/81780
4. Rouvroy G., Standaert FX., Quisquater JJ., Legat. JD., Efficient Uses of FPGA's for implementations of DES and its Experimental Linear Cryptanalysis, In IEEE Transactions on Computers, Special CHES Edition, стр. 473-482, Април 2003.
5. http://www.altera.com/products/ip/ip-index.jsp
6. http://www.cast-inc.com
7. http://www.microsemi.com/
8. http://www.nist.gov/
9. http://www.xilinx.com

ЕДИН МЕТОД ЗА ОЦЕНКА НА ЗАПЛАХИТЕ ЗА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Димитър Т. Дойчинов

Национален Военен Университет "В. Левски",
Факултет „Артилерия, ПВО и КИС", ул. „Карел Шкорпил" 1, Шумен,
e-mail: d.doychinov@nvu.bg

A METHOD FOR ASSESSING INFORMATION SECURITY THREATS

Dimitar T. Doychinov

ABSTRACT: This paper presents a method for assessing information security threats. Overall guidelines of the method and threat metrics are given.

KEY WORDS: assessing threats, information, security.

При разработването на концепция на система за сигурност на информация един от най-трудните и времеотнемащ процес е анализът на възможните заплахи, последствията от тях и класификацията им по степента на тяхната потенциална опасност.

Предвид целите, преследвани от нарушителите на информационната сигурност, следва да се съсредоточи вниманието върху следните области: нарушаване на поверителността, цялостността и достъпността на защитена информация [3].

Разработването и реализирането на заплахи се влияе от множество фактори от различно естество – икономически, технически, организационни, технологични и други, като може да се изтъкнат следните [1, 2]:

- очакван от нарушителя "ефект " от реализирането на заплахата;
- сложността на проектирането и изпълнението;
- необходимите разходи;
- възможно наказание на нарушителя в случай на идентифициране на заплахите.

В качеството на идентификатор на заплахите се въвеждат следните показатели:

А – нарушени принципи на информационна безопасност:

1 – нарушение на конфиденциалността на служебната, личната и друга конфиденциална информация;

2 – нарушение на целостта и достоверността на съхраняваните данни с помощта на специални програми;

3 – нарушаване на достъпността на системата, данните и услугите за всички оторизирани потребители;

4 – неспазване на закони, разпоредби, лицензи и етични стандарти в използването на информация.

Б – възможността за предотвратяване. Оценява се възможността за предотвратяване на заплахите за конкретната система в реални условия:

1 – лесно; 3 – много трудно;
2 – трудно; 4 – невъзможно.

В - откриване на заплахи - оценка на способността за откриване на заплахи (автоматично или ръчно):

1 – лесно; 2 – трудно; 3 – невъзможно.

Г – възможност за неутрализиране / възстановяване. Оценяват се усилията, необходими за неутрализиране на заплахата (за принципите за безопасност А1) или възстановяване на нормалния режим на работа (за принципите на безопасност А2 и А3):

1 – лесно; 3 – много трудно;
2 – трудно; 4 – невъзможно.

Д - честота на възникване. Тази оценка отразява честотата на възникване на конкретната заплаха в сравнение с други заплахи:

0 – неизвестена; 2 – средна;
1 – ниска; 3 – висока; 4 – свръхвисока.

Таблица 1. Оценка на честотата на възникване на заплахите.

Честота на възникване	Оценка Д
неизвестна	0
1 път годишно	1
10 пъти годишно	2
100 пъти годишно	3
1000 пъти годишно	4

Е - потенциална опасност – оценява се опасността на заплахата се по отношение на щетите, които могат да бъдат нанесени на системата в случай на реализация на заплахата:

1 – ниско; 2 – висока; 3 – свръхвисока.

Ж - източник на заплахата:

1 – вътрешни; 2 – външни.

З - Ниво на необходимите знания. Оценява се нивото на професионална подготовка на нарушителите, необходима за реализирането на съответната заплаха:

1 – фундаментални знания за системната организация, комуникационните протоколи и т.н.;

2 – познаване на операционната система;

3 – владеене на езици за програмиране;

4 – основни познания в областта на изчислителната техника.

Следва да се отбележи зависимостта – колкото е по-високо нивото на знания, необходими за изпълнението на заплахата, толкова по-малко тя е привлекателна за нарушителя. В някои случаи, причинно-следствената връзка не е линейна.

И - разходите за проектиране и разработка на злоупотреба:

1 – големи; 2 – средни; 3 – малки разходи.

К - лекота на изпълнение:

1 – много трудно; 3 – относително лесно;

2 – трудно; 4 – лесно.

Л - потенциалните санкции съгласно действащото законодателство:

1 – тежки наказания (включително и наказателна отговорност);

2 – незначително наказание;

3 – без наказание.

Предлаганата система от символи и оценки, както и съответната скала могат да бъдат детайлизирани за конкретна система в зависимост от характера на дейността, защитаемите ресурси и важна информация.

Комплексната оценка за *i*-тата заплаха $K_i^{'}$ се изчислява, както следва:

$$K_i^{'} = \frac{\sum_{j=1}^{m} \frac{K_{ij} + K_{j\max}}{2}}{m} \qquad (1)$$

където K_{ij} – оценка на *i*-тата заплаха по отношение на *j*-тия параметър; m – брой на параметрите за оценка на *i*-тата заплаха; K_{jmax} – максимална оценка по отношения на j-тия параметър.

Анализ на оценката на заплахите за сигурността показва, че за работата на системата са най-опасни потребителските грешки и целенасочените действия на вътрешни лица. Това се дължи на факта, че тяхното предотвратяване е трудно. Заплахата с най-малка опасност е претоварване на системата. Това се дължи на факта, че е лесна за предотвратяване, ако се организира мониторинг на наличните ресурси на системата и се анализира тяхното използване.

Вероятните заплахи за сигурността е целесъобразно да се разделят на три основни групи [5, 6]:

- неопасни заплахи, които лесно се предотвратяват или разкриват, неутрализират и премахват;

- опасни, за които процесите на предотвратяване, разкриване и неутрализиране на ефектите от технологична гледна точка не са отработени;
- много опасни, които имат максимални оценки по всички параметри, а реализирането на процесите по противопоставяне е свързано със значителни разходи.

Въз основа на проведения анализ е възможно развитието на разгледания подход към описанието на привлекателността на заплахите за нарушителя, който се строи с помощта на следните променливи: $\mathbf{B_0}$ – облагата на нарушителя от реализирането на заплахата, $\mathbf{C_0}$ – разходите на нарушителя за подготовка и реализация на заплахата.

Следователно, колкото е по-голямо съотношението $\mathbf{B_0/C_0}$, толкова по-големи са икономическите основания за изпълнение на заплахата. Тогава показателя за привлекателността на заплаха за нарушителя ϑ е равен на:

$$\vartheta = \frac{Pu.\mathrm{B}_0}{C_0} \qquad (2)$$

където $\mathbf{P_u}$ – усреднената вероятност за успешна реализация на заплаха.

Като част от информация конфликт нарушителят се стреми да разработи/интегрира програмна заплаха с максимален показател на привлекателност ($\vartheta \rightarrow \max$). Основната задача на системата за защита е да предотврати проникването и развитието на заплахата, т.е. минимизиране на дадения показател ($\gamma \rightarrow \min$).

Да разгледаме модела за възможните резултати от взаимодействието на комплекса от заплахи и системата за защита [3]. Междинни състояния в модела могат да бъдат **p1, p2, p3, p4, p5, p6**, описани както следва:

- състояние p1– заплахата е предотвратена, вероятността за такъв изход Pa;
- състояние p2 - заплахата не е предотвратена, вероятността за такъв изход е равна 1 – Pa;
- състояние p3– заплахата е открита, вероятността за такъв изход Pd;
- състояние p4– заплахата не е открита, вероятността за такъв изход 1 - Pd;
- състояние p4– заплахата е неутрализирана, вероятността за такъв изход Pn;
- състояние **p6**– заплахата не е неутрализирана, вероятността за такъв изход $\mathbf{1 - P_n}$.

Състояния в резултат на взаимодействието могат да са събитията **A, B, C** и **D**. Съдържанието им е следното:

- Събитие A – заплахата е предотвратена. Вероятността за такъв изход PA е равна:

$$\boldsymbol{P_A = P_a} \qquad (3)$$

- Събитие B – заплахата не е предотвратена, но е открита и неутрализирана. Вероятността за такъв изход $\mathbf{P_B}$ е равна:

$$\boldsymbol{P_B = (1 - Pa).Pd.Pn} \qquad (4)$$

- Събитие C – заплахата е предотвратена, открита е, но не е неутрализирана. Вероятността за такъв изход $\mathbf{P_C}$ е равна:

$$\boldsymbol{P_C = (1 - P_a).P_a.(1 - P_n)} \qquad (5)$$

- Събитие D – заплахата не е предотвратена и не е открита. Вероятността за такъв изход $\mathbf{P_D}$ е равна:

$$P_D = (1 - Pa).(1 - Pd) \quad (6)$$

Събитията **A** и **B** са благоприятни за системата за защита, а събитията **C** и **D** неблагоприятни, но са благоприятни за нарушителя.

Вероятността за събитие **(A + B)** е:

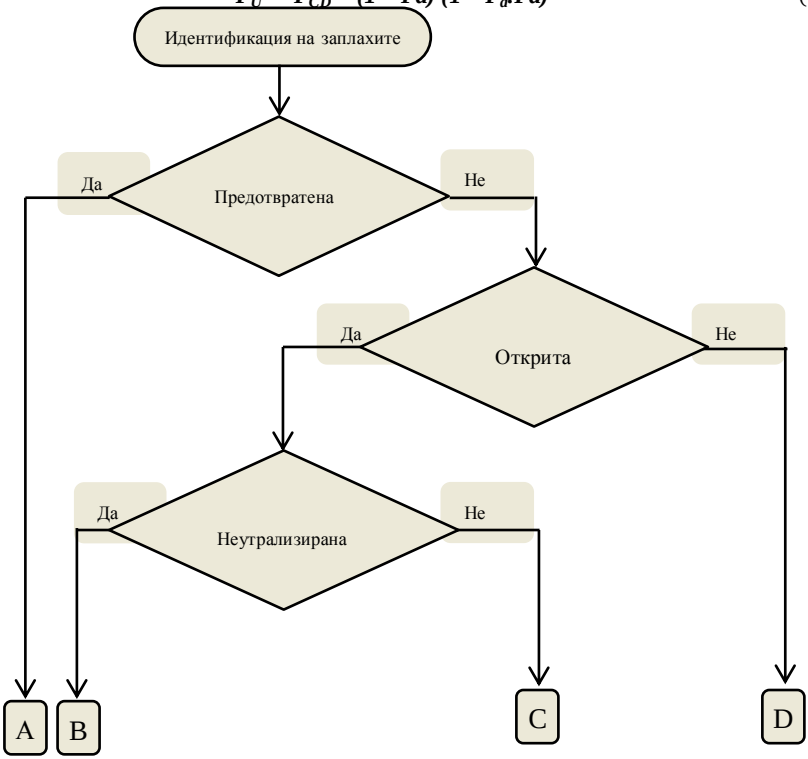
$$P_{AB} = Pa + (1 – Pa).Pd.Pn \quad (7)$$

Вероятността за събитие **(C + D)** е:

$$P_{CD} = (1 – P_a)(P_d (1 – P_n)+ (1 – P_d)) = (1 – P_a) (1 – P_d.P_a) \quad (8)$$

От тук може да се направи изводът, че показателя $\mathbf{P_{CD}}$ в общия случай е и мярка за успешното реализиране на заплахата и е вярно следното равенство:

$$P_U = P_{CD} = (1 – Pa) (1 – P_d.Pa) \quad (9)$$



Фигура. 1. Схема на алгоритъма за анализ на реализирането на заплахите.

Отчитайки равенството 2.8, израза 2.2 приема вида:

$$\vartheta = \frac{(1 - P_a)(1 - P_d P_n)\,\mathrm{B}_0}{C_0} \quad (10)$$

Разгледа се процеса на комбиниране от нарушителя на комплекса от способи и форми на заплахи за достигане на поставената цел. Основните критерии за избор са на основата таблицата с оценки на заплахите от гледна точка на тяхната опасност. Заплахите с най-добри параметри са тези, за които показатели имат следните стойности: **Б = 3** – не може да бъде предотвратено **(P_a = 0)**, **В = 3** – невъзможно да се открие **(P_d = 0)**, в този случай **Е → max**. В този случай привлекателността за нарушителя е очевидна.

Достатъчно условие за реализиране на заплахата е да е изпълнено $C_0 > B_0$, тъй като вероятността за успех на реализацията на заплахата P_U е равна на 1:

$$P_U = (1 - P_a)(1 - P_d.P_n) = (1 - 0)\ (1 - 0.P_d) = 1 \qquad (11)$$

където

$P_a = 0$ – вероятността за предотвратяване на *заплаха*та;

$P_d = 0$ – вероятността за откриване на *заплаха*та от системата за защита;

P_n – вероятността за неутрализация на *заплаха*та.

Тъй като вероятността за неутрализиране на заплахата P_n зависи от наличната информация за заплахата, може да се твърди, че колкото е по-малък обема на информация за заплахата, толкова по-малка вероятността, че в системата за защита ще съществуват разработени механизми за откриването и неутрализирането ѝ. С други думи, когато $P_d \to 0$ имаме $P_n \to 0$. В този случай е вярно твърдението, че $P_n \le P_d$.

Тогава израз 10 придобива вида:

$$\vartheta = \frac{B_0}{C_0} \qquad (12)$$

Формулираме условията за привлекателност на заплаха за нарушителя (данните са представени в низходящ ред по приоритет):

- Б → max. В този случай се предполага реализирането на заплаха, която не може да бъде предотвратена от системата за защита. Колкото показателя Б е по-голям, толкова по-голяма е вероятността заплахата да бъде реализирана. Ако Б = 3, заплахата не може да се предотврати;
- В → max. Случай на реализиране на заплахи, които не могат да бъдат открити или за които дадения показател е близък до максималната стойност.

От гореизложеното може да се направи извод, че при реализирането на новите заплахи, които системите за защита не предотвратяват и не откриват, основният фактор, влияещ върху решението на нарушителя е отношението приходите към разходите. В този случай, при определянето на стойността на активите на информационната система трябва да се вземе под внимание, че извършителят може да се използва система за оценка, различна от тази на собственика на активите, както и цената на атакуваните ресурси на информационната система на черния пазар, което оказва значително влияние върху решението за прилагане на заплахата.

Литература:

1. Ortalo R., Y.Deswarte, Quantitative Evaluation of Information System Security
2. Peltier T. R., Justin Peltier, John Blackley, Managing A Network Vulnerability Assessment, Auerbach, 2003

3. Peltier, Thomas R. Information Security Fundamentals, Second Edition, CRC Press 2013
4. Rathaus N, Vulnerability assessment, white paper, достъпно от: http://www.beyondsecurity.com/pdf/AVDS_Whitepaper.pdf
5. Stoneburner G., Goguen A., Feringa A., Risk Management Guide for Information Technology Systems, NIST, 2002
6. Visintine V., An Introduction to Information Risk Assessment GSEC Practical, Version 1.4b August 8, 2003

ЕФЕКТИВНОСТ НА СОФТУЕР ЗА КОМУНИКАЦИОННО РАЗУЗНАВАНЕ

Линко Г. Николов, Красимир О. Славянов

Национален военен университет „Васил Левски"
Факултет „Артилерия. ПВО и КИС", гр. Шумен

BENEFITS AND FEATURES OF A COMINT SOFTWARE

Linko G. Nikolov, Krasimir O. Slavianov

***ABSTRACT**: Software modules are used as core components in advanced radiomonitoring and radiolocation systems. A COMINT software covers a broad scope of functions. Systems using COMINT software are intended for government authorities entrusted with public safety and security missions and for the armed forces. The graphical user interface is in favor of the commander and/or the decision maker.*

***KEY WORDS**: communication intelligence – COMINT, signal intelligence – SIGINT, electronic intelligence – ELINT, direction finder, communications order of battle – COB, not-of-interest frequency - NOIF*

1. Увод

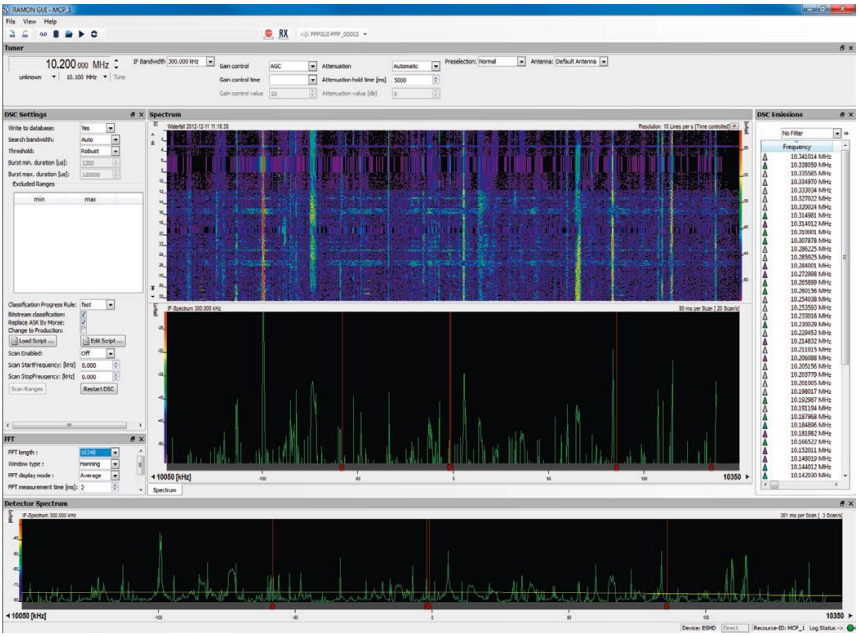
Един софтуер за сигнално разузнаване може да се състои от няколко модула с различни функции. Модулите на този софтуер се явяват основни ядра в системите за радионаблюдение и радиолокация. Различните функции на софтуера могат да бъдат:

- компютърно управление на оборудването;
- съхранение и анализиране на получените данни от оборудването;
- управление и наблюдение на информационния поток в мрежова система, обхващаща множество работни станции;
- улесняване на изпълняваните задачи чрез пълна автоматизация и др.

Системите, използващи завършен софтуер за радионаблюдение, са предназначени за държавни институции, осигуряващи обществена сигурност и защита. Такива системи се предоставят от фирмите производители като цялостно решение, покриващо широк спектър от задачи, като:

- събиране на информация, определяща политически решения;
- гранична защита (предотвратяване на контрабанден внос и незаконно преминаване);
- персонална и имотна защита;
- поддържане на военни операции като мироналагане и мироопазване, чрез откриване на застрашаващи мисията факти или защита на собствените сили и др.;

Оборудването за радионаблюдение и радиолокация, заедно с IT компоненти и комуникационна инфраструктура, се привързват в единна мрежова архитектура чрез софтуера от модулен тип, който осигурява интерфейс за потребителите (фиг.1). [2]



Фиг. 1. R&S®RAMON графичен потребителски интерфейс (GUI) на R&S®CA120 мултиканална система за анализ на сигнали: широколентов спектър и списък от излъчвания, получен от детектор за конвенционални радиосигнали.

Основните функционални предимства, към които се насочват производителите на системи за сигнално разузнаване, са:

- пълен обхват от изпълнявани задачи;
- висока вероятност за прихващане на широка гама сигнали;
- възможност за надграждане и гъвкаво изменение на системата;
- мобилност и комуникационна съвместимост;
- планиране на извършваните задачи;
- автоматизация на радионаблюдението;
- засичане на радио мрежи и извършване на оценка;
- единно управление на експлоатацията на системата;

- вграждане в мрежово-центрични бойни системи (C4ISR);
- предлагане на завършено цялостно решение по предпочитания на клиента. [1, 2]

В основата на софтуера стои процеса на разузнаване. Разузнаването може да се определи като получаване на познания относно света наоколо, което ще допринесе цивилните и военните ръководители на дадена държава да вземат информационно издържани политически и военни решения. Единия от методите за извършване на информационно разузнаване е прослушването на радиоефира и комуникационните мрежи – сигналното разузнаване (SIGINT). Сигналното разузнаване прихваща комуникации и електронно предаване на данни и може да се раздели на два дяла – комуникационно разузнаване (COMINT) и електронно разузнаване (ELINT).

Разузнавателна информация се придобива след извършването на няколко стъпки от кръгов процес, включващ планиране/насочване, събиране, обработване, анализ и разпространяване на информация. Всички тези стъпки трябва да са предвидени от разработчиците на софтуера, с цел да се постигне пълен обхват от мероприятия. Кръговият процес определя обратна връзка, чрез която се оценява степента на ефективност на сигналното разузнаване и до каква степен са изпълнени поставените изисквания (фиг. 2).

Фиг. 2. Разузнавателен цикъл

2. Функционалности на софтуер за сигнално разузнаване

Сигналното разузнаване се явява част от единния процес на информационното разузнаване и също може да се представи като кръгов процес, включващ: планиране на задачите, прихват на сигнали, възпроизвеждане в разбираем режим, технически/съдържателен/тактически анализ, препращане и разпространяване на информацията (Фиг.3).

Според обема на системата за комуникационно разузнаване, стъпките в този кръгов процес могат да се изпълняват от един или няколко оператора чрез подсистеми. Планирането на мисията за сигнално разузнаване включва планиране броя и местонахождението на развърнатите мобилни станции и създаване на заповеди /задачи/, разпространявани до изпълнителите. Процесът на прихващане включва приемане, определяне посоката на направлението, фиксиране на местоположение и наблюдение на комуникационните сигнали. Към възпроизвеждането спада демоду-

лацията, декодирането и по възможност - декодирането на прихванатите сигнали и данни и последващото им съхранение като аудио-, видео-, снимкови или текстови файлове. Анализирането на информацията става в различни отделения – технически, трафичен, съдържателен и тактически. Техническият анализ в сигналното разузнаване се заключава в оценката и класифицирането на техническите параметри на прихванатия сигнал, които инициализират предавателя. Трафичният анализ осигурява информация за времето на ползване на мрежата, интензивност на обмена, тактическата принадлежност, каква организация е развърната и комуникационното оборудване на опонента. Съдържателният анализ изисква семантична оценка и евентуален превод от чужд език на прихванат гласов файл или данни. Тактическият анализ осигурява преглед на комуникационната картина в акаунт, чрез който тактическите резултати се разпращат до ползвателите на разузнавателната информация. Разпространяването на доклади с получена информация затваря кръга, като се определя полезността, изпълнените задачи и ефективността на системата за комуникационно разузнаване.

Фиг. 3. Цикъл на комуникационно разузнаване

Софтуерът за сигнално разузнаване трябва в пълен обем и с улеснен интерфейс да покрива всички тези изисквания. Комуникационното оборудване като приемници, антени, декодери, дешифратори и др. трябва да могат лесно да се преконфигурират и управляват. Операторите трябва да бъдат улеснявани при анализа на приетата информация, както и много стъпки трябва да бъдат автоматизирани, с цел печелене на време и повишаване на ефективността.

На практика съществуват две различни системи за комуникационно разузнаване: стратегически и тактически.

2.1. Стратегически системи COMINT

Стратегическите системи се използват за добиване на сведения, определящи военната ситуация в други държави и събиране на информация за сигурността в собствената държава. Такава информация се определя като съществена при вземането на политическо или военно решение, което способства за предсказването на съпътстващи кризи още в начален стадий. Стратегическите системи работят продължително преди и по време на кризисни ситуации. От основополагащо значение за системата е наличието на базови данни за сравнение и оценка, което формира

нейната ефективност. Системата покрива голям географски периметър, което може да я класифицира и като национална. Следователно в нея ще работят голям брой станции, персонал и оборудване. Специални компоненти, подпомагащи техническия анализ на прихванатите сигнали, влизат в състава на стратегическите системи. Въпреки че задълбочения технически анализ отнема време, това не представлява проблем за системи от такъв мащаб. Изискването към времевия фактор определя разликата между двата вида системи – стратегически и тактически. Цел на разработваният софтуер е да обедини сензори, работни станции и оператори от различни географски местоположения, за да се получи централизирано управление в единен център за командване и управление (C2).

2.2. Тактически системи CESM

Тактическите системи за сигнално разузнаване се характеризират като сензорни системи на комуникационната и електронна поддръжка (CESM) на силите. Тези системи се използват за придобиване на информация на място. Най-често военен командир е под отговорност за използването им. Пример за функционално използване на CESM са мироопазващите операции на ООН извън територията на собствените войски и сили от дадена държава. Но наред с това може да се посочат и местни конфликти и спешни случаи, застрашаващи обществената сигурност. Придобиването на информация чрез комуникационно разузнаване допринася за оказване на непосредствена помощ и бойна поддръжка. В тактическите системи времевият фактор е от по-голямо значение в сравнение със стратегическите, защото действията се развиват по-бързо и колкото по-бързо се придобие и анализира дадена информация, толкова по успешна ще е мисията. Но въпреки това, няма толкова ясно изразена разграничителна линия между COMINT и CESM. И двете системи зависят една от друга и взаимно се допълват. [2]

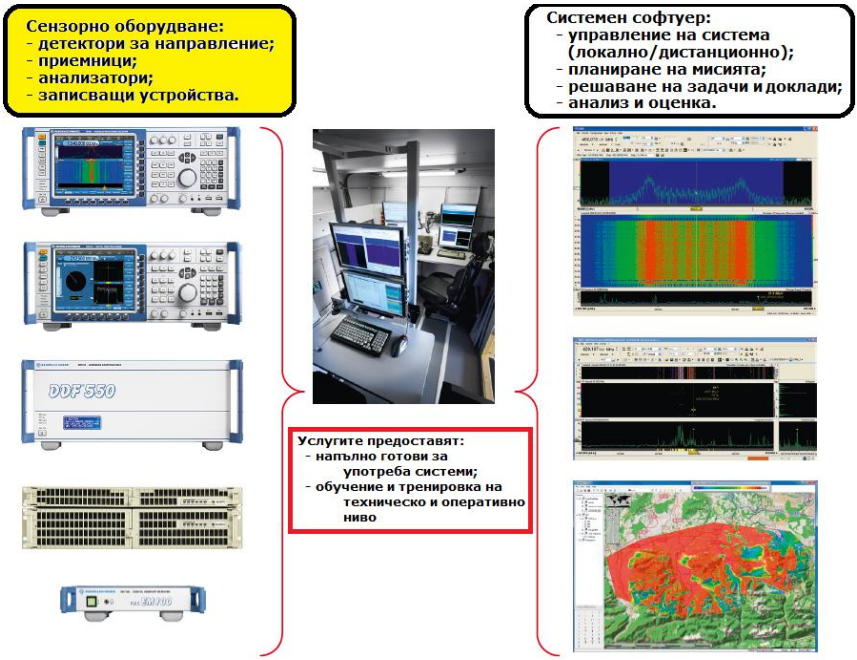
Тактическите системи за сигнално разузнаване се явяват част от цялостния процес по разузнаване. Те са най-вече мобилни, приемниците с антените са инсталирани върху високо проходими машини или на борда на кораби. Географския район на прихват обаче бива ограничен от височината на мачтите, маскировъчните мрежи и укритията на машините. Набляга се на максималната мобилност и въоръжената охрана, защото обектите от системата се разполагат в периметъра на действията.

Работата на тактическите системи се основава на базови параметри за сравнение, получени от стратегическите системи. Резултатите веднага се включват в текущото планиране, включително и в ранното предупреждение на собствените сили, тъй като е налице постоянен натиск от недостиг на време. Поради тази причина, непознати и неизвестни сигнали не се анализират в дълбочина, а вместо това се набляга на базовите познати сигнали. Също така, поради изискването за висока мобилност, численият състав е редуциран. Това определя, софтуерът за сигнално разузнаване да е насочен главно към следене за поява на заплаха в лицето на сигнали от честотни ленти, използвани от противник или дадена целева институция. Затова задълженията на операторите се свеждат до дистанционно наблюдение на автоматизираните процеси, както и експлоатацията на оборудванията и подсистемите.

3. Пълен спектър от COMINT функционалности

Разработчиците, производителите и доставчиците на цялостни, напълно готови за употреба системи за комуникационно разузнаване са готови да предоставят цялостни решения в едно изпълнение, т.е. предлагат цялостно портфолио от ком-

поненти (хардуер и софтуер), както и услуги като управление на проекти, системно инженерство и обучение на потребители, ключови компоненти за една система от такъв характер. Разбира се апаратурата за такъв вид дейност трябва да отговаря на високи изисквания и да включва голям набор от антени за различните честоти (от 100 Hz до 40 GHz), сензори за радиомониторинг и откриване на посоката на разпространение или радиолокация, както и компоненти за анализиране на сигнала. Системния софтуер се състои от широк набор от модули за различни нужди като: планиране на мисията, контрол на всички сензори и потока на информацията с наличното оборудване, анализ, обработка и съхранение на цялата получена и разпозната информация и система за база данни, както и за различни видове отчети. Софтуерните модули най-често се проектират като многофункционални продукти с общо предназначение или commercial off-the-shelf (COTS) (фиг. 4) [2]



Фиг. 4. Съвременна система за радиомониторинг

4. Голяма вероятност за прихващане

Комуникационните системи изключително прецизно и детайлно използват различни методи за разширяване на спектъра. В комбинация с къси, пулсиращи емисии на сигнали правят разкриването на действията възможно най-трудно.

Системите за радиомониторинг и радиолокация са конструирани да се справят високо точно в подобна защитена среда. Големите възможности за разпознаване и разкриване на комуникационната линия правят възможно високо надеждното им действие при сигнали с малка вероятност за прихват или „Low probability of

intercept“ (LTI), както и съхранение на емисията след това с цел декодиране на съобщенията на следващ етап. [3]

Това се постига с използването на широколентови сензори (приемници и детектори на направления) и алгоритми за детекция, които позволяват на потребителя да се запознае дори с най-кратките кореспонденции. Системният софтуер позволява подобни сесии да бъдат отново идентифицирани при повторна детекция на сигнали. За целта софтуера автоматично сравнява изследваните стойности на параметрите с профила на сигнал, който може да се намира в базата данни. Интелигентните методи за компресия на изпратените данни позволяват дистанционно управление на системите за детекция на LTI.

5. Приспособимост и мащабируемост

Мащабируемостта е ключова способност на съвременните системи за радиомониторинг от все по-голяма важност, особено от чисто практична гледна точка. Мащабируемостта и модулната структура на такива системи има своите ключови предимства:

- Системата може да бъде адаптирана и реконфигурирана от потребителя според нуждите му ръчно (в съответствие с текущата мисия);
- Лесно надграждане и осъвременяване за посрещане на променливи изисквания;
- Интерфейси, позволяващи лесна интеграция със съществуващи потребителски архитектури;
- Възможности за дистанционен контрол с използване на всякакъв тип кабелни или безжични комуникационни връзки и различни скорости на трансфер.

6. Мобилност и взаимосвързаност

Тактическите системи за радиомониторинг, в това число и като част от мирообезпечаващи и мироналагаши операции, се използват за постигане на следните цели:

- Идентификация на електронни заплахи;
- Защита на силите;
- Получаване на информация и конкретни данни за планиране на електронната защита, разузнаване и борба.

За постигане на тези цели тактическите системи за радио мониторинг трябва да изпълняват следните изисквания:

- Интеграция във високо мобилни, високо проходими превозни средства;
- Автономно изпълнение на индивидуални подсистеми;
- Мрежова свързаност на множество подсистеми за изграждане на радиолокационната мрежа;
- Връзка с командния контролен център, специализиран център за разузнаване или със системи C4ISR;
- Свързаност с отдалечени станции на театъра на мисията и локални адресати за обмен на доклади. [3, 4]

6.1. Сподобности за дистанционно управление

Способностите за дистанционен контрол е жизнено важна характеристика сред системните компоненти за изграждане на системата за комуникационно информационна поддръжка. Тя е критична в системи, при които множество сензорни подсистеми трябва да комуникират помежду си посредством кабелна или безжична

преносна среда, в това число и при мрежа за радиолокация включваща множество отдалечени детектори за комуникационни направления. [4]

6.2. Мрежова организация

При използването на кабелни или безжични комуникационни връзки без отношение към посоката на комуникацията са характерни следните особености:

Радиостанциите – ако са за военни цели, за тактическо или цивилно приложение най-често позволяват само симплексна комуникация. Предаването на данни посредством широко разгърнати мрежи (WAN) се нуждае от способности за напълно двуканална комуникация. Тези способности се предлагат от съвременните връзки използващи закупени или наети линии от публичната кабелна мрежа, както и от мобилните радиолинии (в това число GSM), радионаправления и сателитни комуникации (INMERSAT, VSAT). [2, 3]

Комуникацията между модулите на софтуерната система за радиомониторинг се базират на TCP/IP протокола. Където е възможна само симплексна комуникация, софтуерните модули в двата края на системата преобразуват TCP/IP пакетите данни в протокол, подходящ за радиопредаване.

При използването на кабелни или безжични комуникационни връзки без отношение към широчината на лентата са характерни следните особености:

Наличната широчина на лентата за предаване на данни при приложения за дистанционен контрол най-често е ограничена. Системите от радионаправления или наети линии обикновено предлагат широколентови връзки, които позволяват предаването на данни в реално време (включително и от радиочестотния спектър на сканиращия приемник или детектора за радионаправления). Теснолентови връзки не са подходящи за такъв тип предаване на данни.

7. Заключение

Оперативните изисквания за една CESM система трябва да отговарят на възможните средства за комуникация. Понякога обаче се налага наличната система за комуникация да бъде заменена с по-мощна, за да отговаря на все по-строгите оперативни изисквания за радиомониторинг. Софтуерната част на една такава система позволява широколентови сензори, които от своя страна създават големи обеми от данни, които да бъдат дистанционно управлявани с използване на ниско скоростни комуникационни връзки. Това обаче няма да изложи на опасност надеждността на едно разузнаване. Единственото ограничение може да настъпи по отношение на времевите характеристики на видео системата за резултата.

Използвана литература:

7. Здравков, З. Методика за проектиране на защитени автоматизирани информационни системи, Научна сесия 2009, Национален военен университет - Факултет “Артилерия, ПВО и КИС”, Сборник научни трудове, ч. I, Шумен, 2010.

8. Интернет адрес: http://cdn.rohde-schwarz.com/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/ARGUS_bro_en_5213-9657-12_v0500.pdf, 01.06.2014 г.

9. Интернет адрес: http://cdn.rohde-schwarz.com/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/RAMON_bro_en_5214-3152-12_v0301.pdf, 01.06.2014 г.

10. Атанасова, Т., Бочева, П. Изкуствен интелект, Варна, 2001, с. 246.

СТЕГАНОГРАФИЯТА В СОЦИАЛНИТЕ МРЕЖИ И В ОНЛАЙН СПОДЕЛЯНЕТО НА СНИМКИ

Веселка Т. Стоянова

Национален Военен Университет „Васил Левски“, Факултет „А,ПВО и КИС“
9700 гр. Шумен , ул.„Карел Шкорпил“ 1
veselka_tr@abv.bg

Steganography in social networks and online photo sharing

Veselka Stoyanova: veselka_tr@abv.bg,

National Military University, Faculty of Artillery, AAD and KIS, 1 Karel Shkorpil Str., 9700 Shumen, Bulgaria

ABSTRACT: *Social networks have created an integrated environment where many different types of communication are possible in the same virtual space. The main aim of present article is based on the study of nature and characteristics of the online social networks and to reveal the most important guidelines for their use in steganography.*

KEY WORDS: *social networks, internet communication, steganography, image*

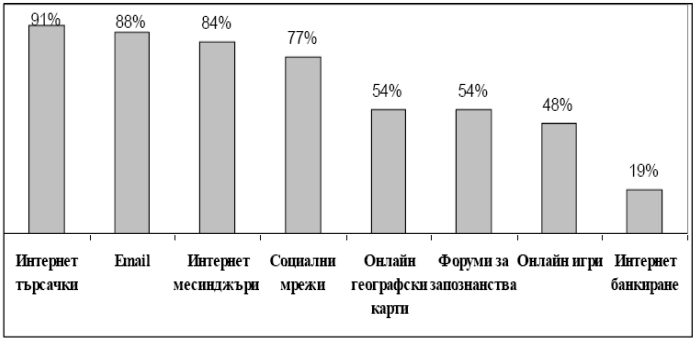
I. Въведение

Развитието и усъвършенстването на информационните и комуникационни технологии съдейства за формирането на глобална цифрова среда, предоставяща нови възможности за осъществяване на лична и бизнес комуникация и взаимодействие, преодолявайки времевите и пространствените ограничения. Непрекъснато нараства броят на потребителите, използващи Интернет за непосредствено споделяне на съдържание и знания, изразяване на мнения, оценки и препоръки в рамките на изградените онлайн социални мрежи и сайтове.

Д. Бойд и Н. Елисон дефинират онлайн социалните мрежи като уеб-базирани услуги, които позволяват на хората да изградят свой публичен или публично-частен профил в рамките на ограничена система, да създадат списък с други потребители, с които те споделят връзки, и да преглеждат списъка от връзки, създаден от други потребители в системата [2]. Социалните мрежи могат да се представят и като конфигурации от хора и/или организации, които са свързани чрез комуникационна среда, формирана от общи интереси, потребности, идеи, убеждения и т.н [5]. По своята същност, това са трите най-важни характеристики, които се отнасят до всяка една онлайн социална мрежа (OSN Online Social Networks), независимо от съществуващите различия относно вида и характера на връзките.

Резултатите от проведеното през 2013 г. национално представително изследване на „Ноема”, потвърждават големия дял на Интернет потребителите, ползващи социалните мрежи като платформа за комуникация и намиране на нови и стари приятели

– 77%. С по-голям процент на проникване са само Интернет търсачките (91%), електронната поща (88%) и т.нар. месинджъри – Skype, ICQ (84%) (вж. Фиг. 1).



Фиг.1. Използвани от българските потребители онлайн приложения през 2013г.[6]

II. Основна част

OSN се основава на представянето на потребителите чрез профили, състоящи се от набор от услуги и социални връзки. Основната услуга предлагана от OSN[те] е създаването на връзки между потребителите, споделящи общи интереси, хобита, спорт, възгледи и други. Тази услуга най-често е свързана със споделянето на изображения. Изображенията могат да бъдат организирани в албуми, да им се прикачи етикет на друг потребител или да бъдат просто така споделени.

Онлайн снимкови услуги (Online Photo Services - OPS) дават възможност да се споделят и управляват изображения в интернет пространството. При тях и при OSN има възможност да се добавят ключови думи за всяка от публикуваните снимки.

Безспорно най-популярните OSN са Facebook и Twetter, като има и други, които са широко разпространени в определени географски области. Например в Северна Америка са популярни MySpace, Google+ и LinkedIn, в Южна и Централна Америка са популярни Orkut и Hi5, в Испания – Tuenti, в Германия StudiVZ, в Канада Nexopia и други.

Уеб сайтовете за OPS дават възможност за публикуване на цифрови изображения и функционалност осигурена чрез приложения подпомагащи потребителите споделянето, визуализацията и управлението на изображенията. В таблица 1 са сравнени някои от най-популярните сайтове за споделяне на снимки по следните показатели:

- ◊ Наименование;
- ◊ Приетия файлов формат по време на споделяне;
- ◊ Възможности за създаване и управление на албуми и директории;
- ◊ Ограничения на предоставяното пространство на потребителя;
- ◊ Има ли възможност за вмъкване на коментари ;
- ◊ Приблизителен брой на регистрираните потребители.

Обичайно OSN и OPS обработват изображенията преди те да бъдат публикувани (преоразмеряване, компресиране, преименуван и др.). Например Facebook променя размера на изображенията с резолюция от 720x720 пиксела до максимална

такава 2048x2048 пиксела. Picasa, разработена от Google, не обработва по никакъв начин публикуваните изображения.

Табл. 1. Сравнение на някои популярни сайтове за онлайн споделяне на снимки

№	Наименование	Формати	Албуми	Размер на пространството	Тагове	Потребители
1.	Flickr	JPEG	Да	3GB	Да	26 000 000
2.	Fotki	GIF JPEG PNG	Да	50MB	Да	1 250 000
3.	Picasa	GIF JPEG PNG	Да	1GB	Да	500 000
4.	Shutterfly	JPEG	Да	неограничено	Не	2 000 000
5.	Windows LivePhotos	JPEG	Да	25GB	Да	56 000 000
6.	Snapfish	JPEG	Не	неограничено	Не	70 000 000
7.	Webshots	JPEG	Не	2GB	Да	32 000 000

Удачно е да се използват възможностите на OSN и OPS, за реализирането на скрита комуникация между две страни, с цел предаване на тайно съобщение. Подходящо е да се използват различи стеганографски техники. Най – простият начин е да се раздели тайното съобщение на части , които да се добавят като коментари към снимки. В този случай е удачно да се използват лингвистична стеганография използваща следните техники [1]:

◊ *Visual Semagram*- невинно изглеждащи образи или физически обекти от ежедневието крият тайното съобщение;

◊ *Text Semagram*- съобщението е скрито така, че да може да се възползва от различните начини а визуализиране на данни;

◊ *Jargon code*- използване на език, разбираем от ограничена група от хора;

◊ *Covered Grille cipher*- използване на шаблон към носителя на скритото съобщение, чрез който символите на скритото съобщение стават видни;

◊ *Covered Null cipher*- съобщението е скрито чрез набор от правила, които са договорени от двете страни , които си комуникират. Например да се четат само първите букви на всяка дума или пък да се четат през пет думи и други подобни условности.

Стеганография в името на файла

Потребителските изображения обикновено се обработват от OSN/OPS преди да бъдат публикувани. Обработката зависи от услугата, обикновено включва някои характеристики на изображението, като формат, размер, метаданни и др.[3]. OSN обикновено правят модификации върху името на файла, който се публикува, а OPS ги оставят непроменени. Затова публикуването на изображение с име следващо общите правила за кодиране използвани в автоматичен режим на именуване на файловете създавани от цифровите фотоапарати не поражда подозрение. Цифровите фотоапарати най-често създават снимки в JPEG формат с задаване на име по

даден шаблон. Размерът на файла зависи от модела на фотоапарата, настройките за компресиране и избраната от потребителя резолюция. Имената на файловете са създадени съгласно шаблони за именуване, които са различни за различните марки устройства, но имат обща черта, която ги обединява и може да се ползва за нуждите на стеганографията, а именно дължина на името, която е от осем знака (xxxxxxxx), последвани от разширението на файла (JPG). В таблица 2 са представени начините на именуване на част от по-известните марки апарати.

Табл. 2. Пример за общото наименуване на част от популярните цифрови фотоапарати

№	Марка	Обичано наименуване на файла	Тип на файла
1.	Canon	IMG_xxxx.JPG	JPEG
2.	Canon (reflex)	iMG_xxxx	RAW
3.	Panasonic, Sony, Nikon	DSC_xxxx.JPG	JPEG
4.	Samsung	SNCxxxxx.JPG	JPEG
5.	Fujifilm	DSCFxxxx.JPG	JPEG
6.	Olympus	P305xxxx.JPG	JPEG
7.	Pentax	IMGPxxxx.JPG	JPEG
8.	Casio	CIMGxxxx.J	JPEG

Всяко име на файла за Panasonic се състои от седем цифри в променливата част на името. Ако отбележим с **K** броя на цифрите и **K<7**, то тогава е необходимо да се използват няколко снимки за да се разпредели съдържанието на информацията за скриване в променливите части на имената на цифровите изображения. Ако **T** е броя на снимките генерирани от същия модел апарат, който е с един и същ шаблон за именуване на файловете, тогава имаме **к.T** десетични знака, които могат да се използват за кодиране на съобщението.

Те съответстват на $\log_2 10^{K.T} \approx 3.32.K.T$ бита.

В този случай скритото съобщение се разпокъсва на няколко части и е важно да се съблюдават точни правила при негово възстановяване.

Някои OSN, като Facebook например, не запазват оригиналното име на файла и го променят с ново, като то вече съдържа стандартна информация (напр. Facebook идентификатор). В този случай не могат да се използват стандартните стеганографски техники. Решение на този проблем може да бъде поле „Описание“ като там се съхрани оригиналното име на вграждания файл и се приложи техника свързана със скриването на информация в името на файла.

Стеганографията с помощта на тагове е метод, който е често използван. „Тагът“ се използва когато потребител на OSN/OPS отбелязва с имена хора, които са на дадена снимка[2]. Потребители прилагащи стеганографията чрез тагове използват набор от снимки публикувани от тях в OSN/OPS, като използват етикетите върху тях, за да кодират скрито съобщение.

Нека се приеме, че потребителя X публикува снимка Y в OSN/OPS и Y_1, Y_2, Y_3,….Y_j са последователност от други снимки, които са част от всички снимки на този потребител. X може да е последователност от потребители X_1, X_2, $X_{3....}$, X_i, които могат да бъдат маркирани в изображенията и така да се скрие информация. Потребителя X може да добавя или не етикет M на всеки потребител X_i. Въз основа на това може да се изгради матрица, която е предложена в таблица 3, където всеки

елемент може: да е 1, ако снимката Y_j на потребителя X_i е маркирана или 0, ако снимката Y_j на потребителя X_i не е маркирана.

Ако се вгради тайното съобщение „This message is hidden” в двоичен код, то ще изглежда по следния начин:

t	h	i	s	
01110100	01101000	01101001	01110011	01000000
m	e	s	s	a
01101101	01100101	01110011	01110011	01100001
g	e		i	s
01100111	01100101	01000000	01101001	01110011
	h	i	d	d
01000000	01101000	01101001	01100100	01100100
e	n			
01100101	01101110			

От таблица 3 се вижда разпределението на байтовете от тайното съобщението в групата от снимки и потребители.

Табл. 3. Матрицата от последователно вградени битове на тайното съобщение

	Снимки										
	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}
X_1	0	1	1	1	0	1	0	0	0	1	1
X_2	0	1	0	0	0	0	1	1	0	1	0
X_3	0	1	0	1	1	1	0	0	1	1	0
X_4	1	0	0	0	0	0	0	0	1	1	0
X_5	1	1	0	1	0	1	1	0	0	1	0
X_6	1	0	1	1	1	0	0	1	1	0	1
X_7	1	1	0	0	1	1	0	1	1	0	0
X_8	0	0	1	0	1	1	0	0	1	1	1
X_9	0	1	1	0	0	1	0	1	0	1	0
X_{10}	0	0	0	0	0	0	1	1	0	1	0
X_{11}	0	1	0	1	1	1	0	0	1	1	0
X_{12}	1	0	0	0	0	0	0	0	1	1	0
X_{13}	1	0	0	0	0	1	1	0	1	0	0
X_{14}	1	0	1	1	0	0	1	0	0	0	1
X_{15}	1	0	0	1	0	0	0	1	1	0	0
X_{16}	1	0	1	0	1	1	0	1	1	1	0

Ако приемем, че един потребител има 11 снимки и 16 приятели във всяка снимка, то цялото съобщение за криене ще е 11*16=176 бита. Съобщението се състои от 22 знака кодирани в ASCII код с един байт, съответно са необходими 176 бита, които да представят съобщението. От таблица 3, която визуализира матрицата на вградените битове се вижда, че на снимка Y_1 трябва да се маркират потребители X_4, X_5, X_6 , X_7, X_{12}, X_{13}, X_{14}, X_{15}, X_{16}, в снимка Y_2 трябва да се маркират потребители X_1, X_2, X_3 , X_5, X_7, X_9, X_{11}, и така до поредна снимка 11. За да се увеличи размера на тайното съобщение може да се публикуват допълнително снимки, а също така да се отбележат и повече потребители (елементи) в нея. За да се подобри ефективността и сигурността е препоръчително да се криптира и компресира вграждената информация. Пример за ефективен алгоритъм за компресиране използван при OSN/OPS е алгоритъмът Deflate[4].

Настройката „Поверителност“ в OSN/OPS повишава степента на поверителност на съобщението, тъй като споделените снимки или албуми с тагове ще бъдат само за определена група от потребители.

Самите социални мрежи, като Facebook, предлагат plug-in, които позволяват вграждането на тайно съобщение в изображение, което се публикува от даден потребител. Тази възможност може се използва, като се инсталира Secretbook чрез Google Chrome. На фиг. 2. се вижда диалоговия прозорец използван при вграждането на тайно съобщение в изображение в приставката на Facebook.

Фиг.2. Secretbook като приложение на Facebook

Secretbook дава възможност да се избере изображение, в което да се скрие тайното съобщение, да се добави парола играеща ролята на ключ и избирайки бутона Create да се създаде стего-изображение.

Видно е, че социалните мрежи предлагат широко поле за употребата на скрита комуникация между множество потребители и добри перспективи за развитие в предвид данните публикувани в фиг.1.

III. Изводи

Повечето OSN/OPS променят публикуваните снимки, поради това не е възможно да се използват класическите методи на компютърната стеганография, затова се търсят и предлагат нови методи за осигуряване на сигурна и скрита комуникация през социалните мрежи. От статията става ясно, че количеството информация скривано чрез компютърната стеганография приложена в OSN/OPS зависи от броя на снимките, споделянето им и възможността за поставяне на етикети, също така определящ е и броя на участващите потребители в комуникацията, именуването им и възможностите за създаване на албуми.

Използвана литература:

1. Bauer F. L., Decrypted secrets - methods and maxims of cryptology (4.ed.). Springer, 2007.

2. Boyd, D., N. Ellison. Social Network Sites: Definition, History, and Scholarship. Journal of Computer–Mediated Communication, 13 (1), article 11, 2007.

Available at: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html [Accessed 23.05.2014).

3. Castiglione A., G. Cattaneo, and A. De Santis, A forensic analysis of images on online social networks, June 2011.

4. Deutsch P.,Deflate compressed data format specification version1.3, https://www.ietf.org/rfc/rfc1951.txt , May 2014

5. Данчев, Д. Концептуални аспекти на интеграцията между социалните мрежи и търговския бизнес. Годишник на Икономически университет-Варна, Варна, Наука и икономика, т. 82, 2010, с. 68.

6. Милев, М. Търсачки и онлайн електронна поща са най-използваните интернет приложения. Noema eBulletin, №5, 2012, с. 1.

МЕТОД ЗА ЧЕСТОТНО РАЗДЕЛЯНЕ НА КАНАЛА ПРИ СИНУСОИДАЛНИ НОСЕЩИ

Атанас И. Начев
Димитър Г. Чобанов

Национален военен университет „Васил Левски"
Факултет „Артилерия. ПВО и КИС", гр. Шумен

METHOD FOR FREQUENCY DIVISION MULTIPLEXING WITH SINUSOIDAL CARRIERS

Atanas I. Nachev
Dimitar G. Chobanov

National military university "Vasil Levski"
Artillery, AAD and CIS faculty, Shumen

Key words: *frequency division multiplexing, orthogonal frequency-division multiplexing*

В доклада е представен метод за честотно разделяне на канала със синусоидални носещи и честотен интервал $\Delta f = \frac{1}{2T}$, при тактов интервал T. Носещите могат да бъдат модулирани по амплитуда и фаза, като фазата може да приема стойности 0 и 180 градуса.

За един тактов интервал модулирания сигнал е:

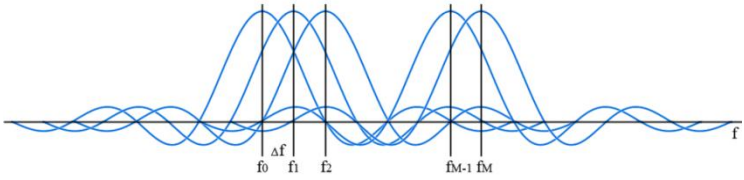
$$S(t) = \sum_{m=0}^{M-1} A_m \sin 2\pi f_m t \qquad 0 \le t \le T \qquad (1)$$

където M е броят на носещите, A_m и f_m съответно амплитуда и фаза на m-та носеща.

Честотата на носещите се изчислява по формулата**:**

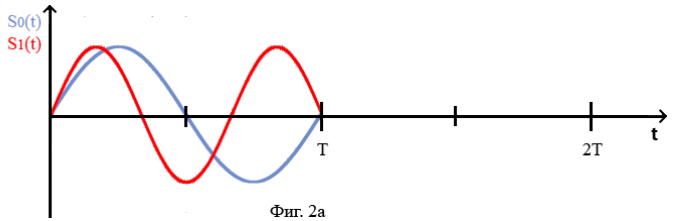
2 $f_m = (P + m)\Delta f$

Спектърът на така формирания сигнал за един тактов период е представен на фиг. 1.

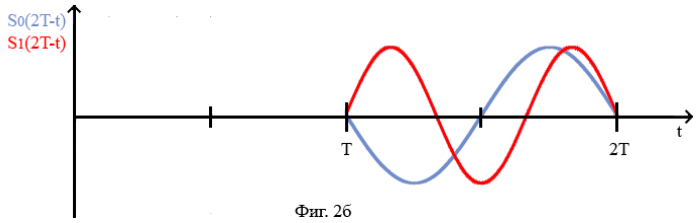


Фиг. 1

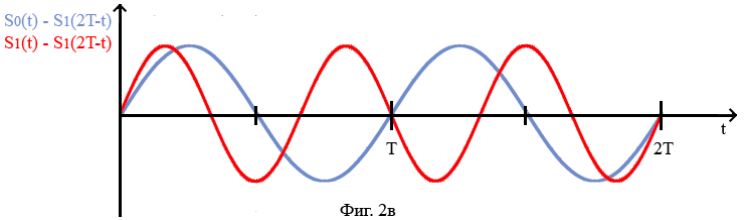
Демодулирането се основава на свойствата на синусоидалната функция. На фиг. 2*а* са представени две носещи – $S_0(t)$ с честота $\frac{1}{T}$ и $S_1(t)$ с честота $\frac{3}{2T}$ при тактов интервал Т. Фиг. 2*б* изобразява огледалното и задържано копие за време 2Т. На фиг. 2*в* е изобразена разликата на оригиналния сигнал и задържаното, и инвертирано във времевата област копие. Сумарният сигнал е с продължителност 2Т (0÷2Т) и разлика между честотите на носещите $\Delta f = \frac{1}{2T}$.



Фиг. 2а



Фиг. 2б



Фиг. 2в

Ще означим със $S_o(t)$ модулирания сигнал S(t), описан във времеви интервал 0÷2Т, а със $S_c(t)$ инвертираното и задържаното във времевата област копие. $S_0(t)$ и $S_1(t)$ се описват както следва:

3 $$S_o\ t\ = \begin{matrix} S(t), & t \in (0 \div T) \\ 0, & t \in (T \div 2T) \end{matrix}$$

(4) $$S_c(t) = \begin{matrix} 0, & t \in (0 \div T) \\ S(2T-t), & t \in (T \div 2T) \end{matrix}$$

Спектърът на сумарния сигнал $S_{\Sigma}(t)$ е:

5 $$S\ f\ = \int_0^{2T} S_o(t)\, e^{-i2\pi ft} dt - \int_0^{2T} S_c(t)\, e^{-i2\pi ft} dt$$

С отчитане на (3) и (4) се получава:

6 $S\ f\ = S_o\ f\ - S_c(f)$, където:

7 $$S_0\ f\ = \int_0^T S\ t\ e^{-i2\pi ft} dt$$

8 $$S_c\ f\ = \int_T^{2T} S(2T-t) e^{-i2\pi ft} dt$$

Полагайки в (8) $l = 2T - t$ и извършвайки необходимите математически операции се получава:

9 $$S_c\ f\ = e^{-i2\pi f 2T} \int_0^T S(l) e^{i2\pi fl} dl$$

Спектъра на сумарния сигнал е:

10 $$S\ f\ = \int_0^T S\ t\ e^{-i2\pi ft} dt - e^{-i2\pi f 2T} \int_0^T S(t) e^{i2\pi ft} dt$$

В (10) полагаме $f = k\Delta f$:

11 $$S\ k\Delta f\ = \int_0^T S\ t\ e^{-i2\pi \Delta ft} dt - \int_0^T S(t) e^{i2\pi \Delta ft} dt$$

Входният сигнал S(t) (1) се дискретизира с интервал на дискретизация t_s. При N дискрети интервала на дискретизация е:

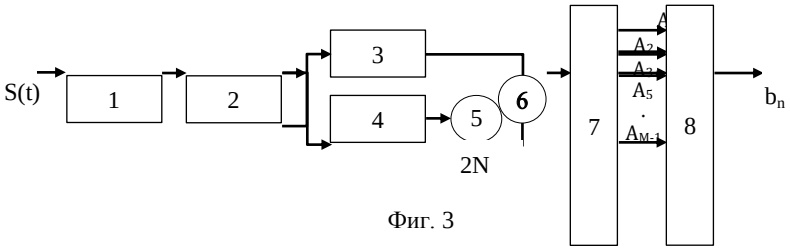
12 $$t_s = \frac{T}{N}$$

След заместване на (12) в (11) се получава:

13 $$S\ k\Delta f\ = \sum_{n=0}^{2N-1} S(nt_s) e^{-i\frac{2\pi kn}{2N}} - \sum_{n=0}^{2N-1} S(nt_s) e^{i\frac{2\pi kn}{2N}}$$

В (13) първата сума е право дискретно преобразуване на Фурие, а втората с точност до множител 2N е обратно дискретно преобразуване на Фурие [1].

Блоковата схема на демодулатора е представена на фиг. 3,



Фиг. 3

където:

- Блок 1 извършва аналогово–цифрово преобразуване
- Блок 2 добавя към дискретизирания сигнал N броя нули
- Блок 3 извършва 2N – точково бързо дискретно преобразуване на Фурие (FFT)
- Блок 4 извършва 2N – точково бързо обратно дискретно преобразуване на Фурие (IFFT)
- Блок 5 извършва умножение с 2N
- Блок 6 извършва изваждане на резултатите от FFT и коригиранот IFFT
- Блок 7 отделя от сумарния резултат стойностите за честоти $f_0 \div f_{M-1}$
- Блок 8 извършва паралелно-последователно преобразуване

Литература:

[1] У. Сиберт. Цепи, сигналы, системы.Москва. „Мир“1988.

МОДЕЛ НА СИСТЕМА С ЧЕСТОТНО РАЗДЕЛЯНЕ НА КАНАЛА ПРИ СИНУСОИДАЛНИ НОСЕЩИ И АМПЛИТУДНО–ФАЗОВА КОРЕЛАЦИОННА МОДУЛАЦИЯ

Димитър Г. Чобанов

Национален военен университет „Васил Левски”
Факултет „Артилерия. ПВО и КИС”, гр. Шумен

MODEL OF SYSTEM WITH FREQUENCY - DIVISION MULTIPLEXING WITH SINUSOIDAL CARRIERS

Dimitar G. Chobanov

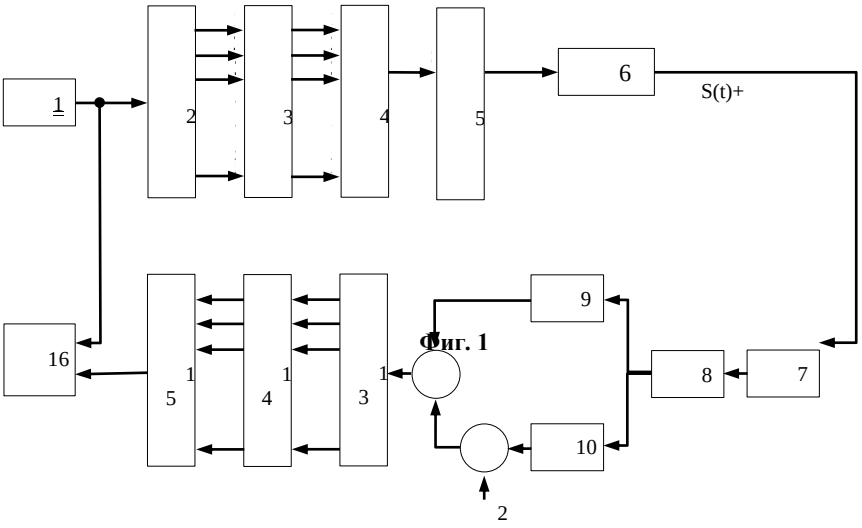
National military university “Vasil Levski”
Artillery, AAD and CIS faculty, Shumen

Key words: *frequency division multiplexing, orthogonal frequency-division multiplexing, AWGN, BER, BPSK, ASK,Matlab, simulation, Simulink.*

В доклада е представен модел на система за честотно разделяне на канала при синусоидални носещи с амолитудно-фазова корелационна модулация. Представени са получените от симулация резултати за вероятността за грешки при предаването на битове (BER).

На основата на алгоритъма за демодулиране на в ситема с честотно разделяне на канала при синосуидални носещи [1] и метода за амплитудно - фазова корелационна модулация [2] е синтезиран модел на система за честотно разделяне на канала при синосуидални носещи Фиг.1. Предназначението на блоковете в модела е следното:

- Блок 1 – генератор на случайна двойчна поредица с равномерно разпределение
- Блок 2 – последователно – паралелен преобразутел
- Блок 3 – модулатор на двоичната поредица
- Блок 4 – модулатор на носещите
- Блок 5 – корелационен филтър
- Блок 6 – канал с адитивен гаусов бял шум
- Блок 7 – аналого – цифров преобразувател
- Блок 8 – формировател
- Блок 9 – право дискретно преобразувание на Фурие
- Блок 10 – обратно дискретно преобразувание на Фурие
- Блок 11 – умножител
- Блок 12 – суматор
- Блок 13 – демултиплексор – селектор
- Блок 14 – прагов детектор
- Блок 15 – паралелно – последователен преобразутел
- Блок 16 – изчислител на вероятността за грешка



Фиг. 1

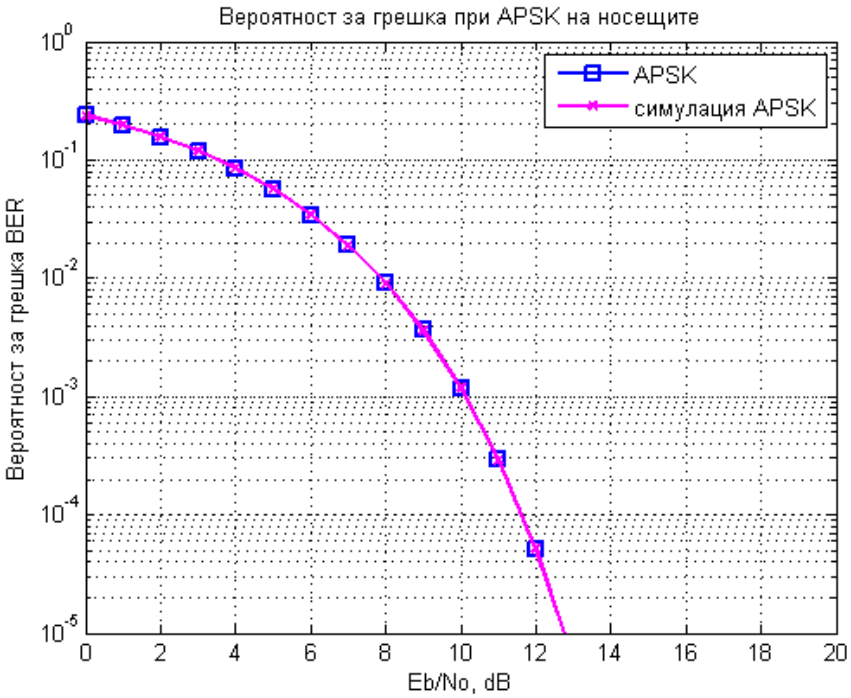
Вероятноста за грешка се изчислява като отношение на броя на сгрешените битове N_{err} към броя на предадените N (1).

1 $$BER = \frac{N_{err}}{N}$$

Теоретичната вероятност за грешка при двоична амплитудна модулация на носещите е:

2 $$BER_{APSK} = \frac{3}{4}\text{erfc}\ \ \overline{\frac{E_b}{2N_0}}\ \ -\frac{1}{4}erfc\ \ 3\ \ \overline{\frac{E_b}{2N_0}}$$

На фигура 2 са представени теоретичната и получената от симулация вероятност за грешка (BER) при двоична амплитудно-фазова корелационна модулация.



Фиг. 3

Литература:

[1] Д. Чобанов. Метод за честотно разделяне на канала при синусоидални носещи

[2] Д. Добрев. Цифрови радиорелейни станции. Методи и устройства. София. ДИ “Техника“.1987

[3] У. Сиберт. Цепи, сигналы, системы.Москва. „Мир“1988

МОДЕЛ НА СИСТЕМА С ЧЕСТОТНО РАЗДЕЛЯНЕ НА КАНАЛА ПРИ СИНУСОИДАЛНИ НОСЕЩИ

Димитър Г. Чобанов

Национален военен университет „Васил Левски”
Факултет „Артилерия. ПВО и КИС”, гр. Шумен

MODEL OF SYSTEM WITH FREQUENCY - DIVISION MULTIPLEXING AND SINUSOIDAL CARRIERS

Dimitar G. Chobanov

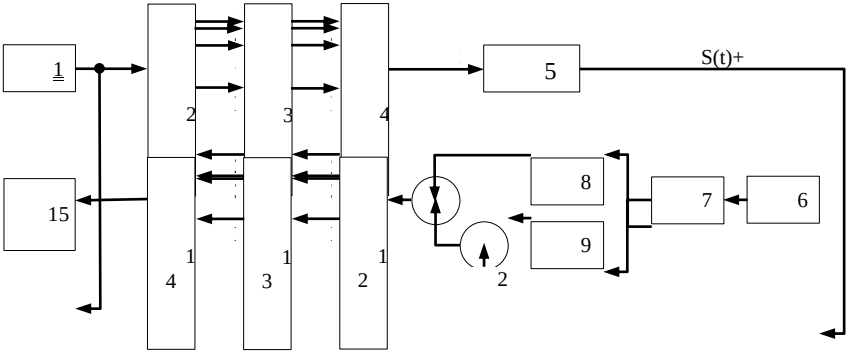
National military university “Vasil Levski”
Artillery, AAD and CIS faculty, Shumen

Key words: *frequency division multiplexing, orthogonal frequency-division multiplexing, AWGN, BER, BPSK, ASK,Matlab, simulation, Simulink.*

В доклада са представени модел на система за честотно разделяне на канала при синусоидални носещи с двоична амплитудна модулация (OOK), и модел на система с честотно разделяне при синосуидални носещи с двоична фазова модулация (BPSK). Представени са получените от симулации резултати за вероятността за грешки при предаването на битове (BER) при OOK и BPSK.

На основата на алгоритъма за демодулиране в система с честотно разделяне на канала при синосуидални носещи [1] е синтезиран обобщен модел на система за честотно разделяне на канала при синосуидални носещи Фиг.1. Предназначението на блоковете в модела е следното:

- Блок 1 – генератор на случайна двойчна поредица с равномерно разпределиние
- Блок 2 – последователно – паралелен преобразутел
- Блок 3 – модулатор на двоичната поредица
- Блок 4 – модулатор на носещите
- Блок 5 – канал с адитивен гаусов бял шум
- Блок 6 – аналого – цифров преобразувател
- Блок 7 – формировател на
- Блок 8 – право дискретно преобразувание на Фурие
- Блок 9 – обратно дискретно преобразувание на Фурие
- Блок 10 – умножител
- Блок 11 – суматор
- Блок 12 – демултиплексор – селектор
- Блок 13 – прагов детектор
- Блок 14 – паралелно – последователен преобразутел
- Блок 15 – изчислител на вероятността за грешка



Фиг. 1

Вероятноста за грешка се изчислява като отношение на броя на сгрешените битове N_{err} към броя на предадените N (1).

$$\mathbf{1} \qquad BER = \frac{N_{err}}{N}$$

При двоична амплитудна модулация на носещите блок 2 извършва модулиране по амплитуда като на логическа нула съответства ниво 0, а при логическа единица ниво $\overline{E_b}$, където E_b е енергията на един бит. Блок 13 извършва сравнение с прагово ниво $\frac{\overline{E_b}}{2}$

Теоретичната вероятност за грешка при двоична амплитудна модулация на носещите е:

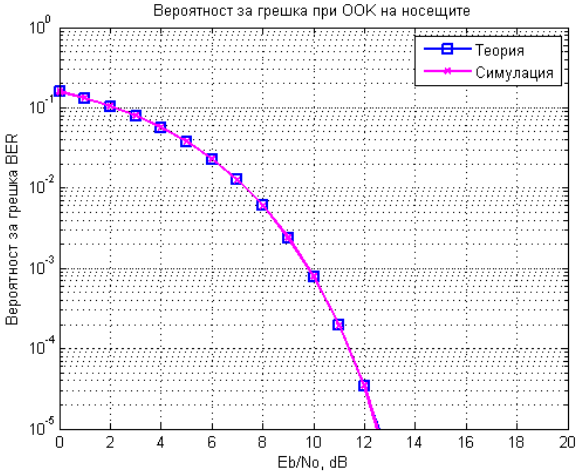
$$\mathbf{2} \qquad BER_{ASK} = \frac{1}{2}\operatorname{erfc}\ \frac{1}{2}\ \frac{\overline{E_b}}{N_0}$$

При двоична фазова модулация на носещите блок 2 извършва модулиране по фаза като на логическа нула съответства ниво $-\ \overline{E_b}$, а при логическа единица ниво $\overline{E_b}$, където E_b е енергията на един бит. Блок 13 извършва сравнение с прагово ниво 0.

Теоретичната вероятност за грешка при двоична фазова модулация на носещите е:

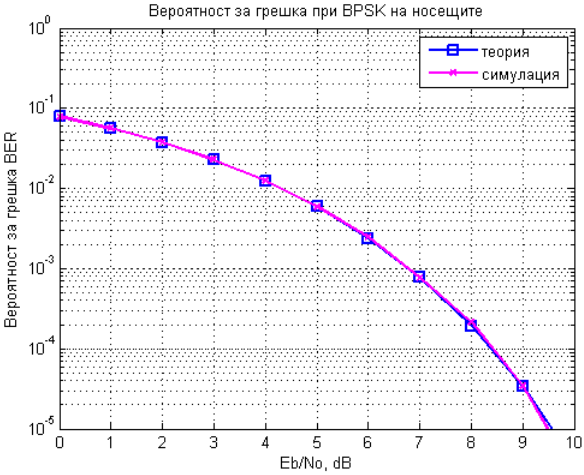
$$\mathbf{3} \qquad BER_{BPSK} = \frac{1}{2}\operatorname{erfc}\ \frac{\overline{E_b}}{N_0}$$

На фигура 2 са представени теоретичната и получената от симулация вероятност за грешка (BER) при двоична амплитудна модулация.



Фиг. 2

Резултатите за двоична фазова модулация на носещите са преставени на фиг. 3.



Фиг. 3

Получените резултати са безспорно доказателство за адекватността на теоретичните и на симулационните модели.

Литература:

[1] Д.Чобанов. Метод за честотно разделяне на канала при синусоидални носещи
[2] У. Сиберт. Цепи, сигналы, системы. Москва. „Мир“1988

СПЕКТРАЛЕН АНАЛИЗ НА СЛОЖЕН (ШУМОПОДОБЕН) РАДИОКАЦИОНЕН СИГНАЛ

Николай Ж. Кулев
НАЦИОНАЛЕН ВОЕНЕН УНИВЕРСИТЕТ " В.ЛЕВСКИ ",ФАКУЛТЕТ „АРТИЛЕРИЯ, ПВО И КИС", ГР. ШУМЕН, УЛ. КАРЕЛ ШКОРПИЛ №1

CORRELATION ANALYSIS OF COMPLEX PHASE MANIPULATED SIGNAL

***ABSTRACT**: It is done an analysis of fifteen-element phase manipulated signals that are applied in the radio location. The analysis is done by a systematic system of criteria and prove their good qualities.*

Задачата за определяне на корелационните и спектралните характеристики на сигналите има определено теоретично значение и практическа полезност, поради еднозначната връзка на спектъра на сигналите с автокорелационната им функция (АКФ) и необходимостта от познаване на ширината на честотната лента и базата на сигналите.

Всеки сигнал може да се представи във времевата и в честотната област, като връзката между тези представяния на сигнала е еднозначна чрез преобразуванията на Фурие. Корелационните функции са свързани с времевата функция на сигнала, а определяща между спектралните му характеристики е амплитудно-честотната характеристика (АЧХ).

АЧХ определя енергетичния спектър на сигнала, чрез който се определя широчината на честотната му лента. Чрез нея се определя базата на радиолокационния сигнал, разглеждана от много автори като критерий за потенциалните възможности и информативност на сигнала, но и като ограничителна характеристика за практическата му реализация със зададена точност.

Спектърът на сигнала е и определяща характеристика при практическата реализация на конкретни устройства.

Към задачата за определяне на спектралните характеристики на сложен (шумоподобен) сигнал могат да се приложат няколко подхода:

- Изразяване на АКФ посредством отрези от прави и използване на класическата зависимост на Винер-Хинчин:

$$S\ jf\ =\ \int_{-\infty}^{\infty} R\ \tau\ .\exp\ -j2\pi f\tau\ d\tau \qquad (1)$$

Тук границите на интегриране следва да се изберат между точките на апроксимация на АКФ с прави линии.

Съществува пълна аналогия между преобразуванията на Фурие и на Винер-Хинчин, откъдето следва и еднозначна връзка между АКФ и спектралната функция на сигнала.

- Прилагане на правото Фурие преобразувание:

$$S\ jf\ =\ \int_{-\infty}^{\infty} S\ t\ .\exp\ -j2\pi f t\ dt \qquad (2)$$

Сложността на аналичния израз за S(t) определя ефективността на този метод за спектрален анализ на сложни сигнали и изискването за подходящо програмно осигуряване.

- Използвайки свойството линейност на честотните спектри, спектърът на сложния сигнал може да се определи като сбор от спектрите на съставящите го елементарни сигнали:

$$S\ jf\ =\ \sum_{i=1}^{N} S_i(jf) \qquad (3)$$

където: $S_i(jf)$ е комплексния спектър на i- тия елементарен сигнал в състава на сложния сигнал.

В някой случаи е целесъобразно определяният спектър да се търси като разлика от спектри на сигнали.

Този подход е много подходящ за спектрален анализ на сложни радиолокационни, впредвид ограничената им продължителност сигнали, тъй като приложимостта му се ограничава не толкова от сложността на сигнала като конструкция, колкото от броя на по-елементарните сигнали с известен или по-лесен за определяне спектър, на които може да се разложи, като най-често има връзка между двете.

Едни от най-значимите за радиолокацията са фазоманипулираните сигнали (ФМС), в частност синалите с двоична фазова манипулация. Към по-съществените аргументи за избора и приложимостта им са: голяма база, откъдето следва възможността за увеличаване на разрешаващата способност по една от координатите на целта, при запазване на висока разрешаваща способност по другата; възможност за работа с ниски спектрални плътности; висока шумозащитеност, която е пропорционална на базата на сигнала; много добри корелационни свойства в честотно-временната област при подходящ избор на кодова последователност (КП); възможност за създаване на голям брой варианти на сигнала при един и същ брой елементарни сигнали (чипове) в структурата му; относително проста реализация на устройствата за формиране и демодулация.

Най-често се приема ФМС да се описват чрез КП, смисълът на което е опростяване на изчисляването на корелационния интеграл, което е основна операция при приемането на сложни сигнали. В търсене на КП с много добри корелационни свойства и с дължина, подходяща за радиолокационен сигнал с оглед на тактическите характеристики на РЛС, в [4] е извършен сравнителен корелационен анализ на петнадесетелементна КП (N=15), получена чрез разширение на 13-елементния код на Баркер с два допълнителни елемента, и М-последователности с N=15, намерили приложение в типови РЛС. Изпозван е избран подбор от следните критерии: максимално ниво на страничен лист на АКФ, отношение на нивата на максималния страничен лист и на главния лист в АКФ, отношение на средноквадратичното ниво на страничните листи и нивото на основния лист на АКФ, брой на блоковете в КП, баланс на фазовия код. Всеки от тези критерии е съществен в радиолокацията в зависимост от характера на изпълняваните тактически задачи.

Основният извод от направения анализ е, че с изключение на баланса на фазовия код, по всички останали критерии, КП { -1 -1 1 1 1 1 1 -1 -1 1 1 -1 1 -1 1 } е с по-добри корелационни свойства от М-последователностите { 1 1 1 1 -1 -1 -1 1 -1 -1 1 1 -1 1 -1 } и { 1 1 1 1 -1 1 -1 1 1 -1 -1 1 -1 -1 -1 }.

Аналитичното описание на ФМС с предложената КП има вида:

$$S\ t\ =\ U_0\ \sum_{k=1}^{15} -1\ ^{d_k}.rect\ t-(k-1)\tau_0\ \cos[\omega_0 t+\varphi_0], t\in[0,T] \qquad (4)$$

където:

$T = N\tau_0$; τ_0 – продължителност на елементарния сигнал в състава на ФМС; U_0 – амплитуда на чипа; ω_0 – носеща честота; φ_0 – начална фаза; $t_k = (\text{к} - 1)\tau_0$ – закъснение на к-тия чип.

Функцията на среда се дефинира:

$$rect\ t-(k-1)\tau_0 = \begin{matrix} 1 \text{ при } (k-1)\tau_0 \leq t \leq k\tau_0 \\ 0 \text{ при } (k-1)\tau_0 > t > k\tau_0 \end{matrix}$$

$$d_k = 0{,}1\ ;\ d_3 = d_4 = d_5 = d_6 = d_7 = d_{10} = d_{11} = d_{13} = d_{15} = 1;$$

$$d_1 = d_2 = d_8 = d_9 = d_{12} = d_{14} = 0;$$

Спектралният анализ на сигнала е направен с прилагане свойството линейност на честотните спектри. Важен допълнителен аргумент в полза на използването на такъв метод за спектрален анализ е обстоятелството, че синтезираните сигнали са крайна последователност от не голям брой чипове с еднаква продължителност във времето τ_0 и еднаква честота на високочестотното си запълване.

Комплексният спектър на к-тия радиоимпулс от излъчвания радиолокационен сигнал може да бъде записан във вида:

$$S_k\ jf = S_1(jf)\ \exp\{-j2k\pi f\tau_0\} \quad (5)$$

където: $k\tau_0$ е закъснението на к-тия радиоимпулс спрямо първия при времево представяне.

Амплитудния спектър $S_1(jf)$ на правоъгълен радиоимпулс с продължителност τ_0 и с неизменна носеща честота f_0 има следното аналитично представяне:

$$S_1\ f = \tau_0\ \sin c\ \pi(f-f_0)\tau_0 \quad (6)$$

За да се предотвратят фазови изместванията при преход от един радиоимпулс към друг в структурата на сондиращия сигнал, носещата честота и продължителността на чипа трябва да са свързани с определена зависимост. Тя следва да се определи от условието:

$$\Psi\ t = \int_0^{\tau_0} 2\pi f t.dt = q.2\pi \quad (7)$$

където: q – естествено число

Прилагайки свойството на спектрите известно като теорема на закъснението и след отчитане на (3), амплитудния спектър на ФКМС може да бъде представен във вида:

$$S(jf) = S_1(jf)\ .\ S'(jf) \quad (8)$$

където: $S'(jf)$ е спектърът на сбора от експоненциалните членове отразяващи измененията на фазите на спектралните съставни в резултат на времевото закъснение на радиоимпулсите след първия.

За анализирания ФМС :

$$S\ jf = \sum_{k=1}^{15} C_k.\exp\{-j2\pi f(k-1)\tau_0\} \quad (9)$$

където: $C_k = \exp\ jd_k\pi$

Следователно амплитудният спектър на сигнала се определя от зависимостта:

$$S\ jf = \tau_0^{\ 1\ 2}\ \frac{\sin\pi(f-f_0)\tau_0}{\pi(f-f_0)\tau_0}\ .\ S'(jf) \quad (10)$$

където:

$$S'(jf) = \left(\sum_{k=1}^{15} C_k.\cos 2\pi f\ k-1\ \tau_0\right)^2 + \left(\sum_{k=1}^{15} C_k.\sin 2\pi f\ k-1\ \tau_0\right)^2\ ^{\frac{1}{2}}$$

Съгласно възприетата методика за спектрален анализ, на базата на (10) е определен амплитурният спектър при следните изходни данни: $\tau_0 = 0{,}4.10^{-6}\ s;\ f_0 = 10.10^9\ Hz.$

В резултат на извършения спектрален анализ на предложения сложен сигнал, могат да се направят следните по-важни изводи:

- анализираният сигнал са широколентови, а амплитудният му спектър наподобява този на шумоподобен сигнал, което следва да се очаква виредвид особеностите на автокорелационната му функция;
- Сравнението на амплитудните спектри на единичен правоъгълен радиоимпулс с неизменна носеща и на ФМС показва, че видът на АЧХ се определя от първия множител в (10);
- Нулите на спектралната плътност на сигнала са разположени по честотната ос при честоти $f_0 \pm \frac{k}{\tau_0}; k = 1,2,3,...;$
- Флуктуациите в АЧХ съществено зависят от втория множител в (10), т.е. от приетият фазов код и броя N на елементите му.
- Обвиващата на амплитудния спектър на периодичен сигнал има аналогичен характер на изменение, но самият спектър е линеен, като разстоянието по честотната ос между съседни спектрални линии е $\Delta f = \frac{1}{N\tau_0} = \frac{1}{15\tau_0}$, което е в съответствие с теоремата на Котелников в нейното честотно представяне.
- Видът на амплитудния спектър на сигнала показва, че енергията му е съсредоточена в честотния интервал:

$$\Delta F = \left| f_н + \frac{1}{\tau_0} \right| - \left| f_н - \frac{1}{\tau_0} \right| = \frac{2}{\tau_0},$$

който с достатъчна степен на точност може да се разглежда като ширина на честотния му спектър, приемайки че в последния е съсредоточена около 90% от цялата енергия на сигнала.

- Изхождайки от определението за база на сигнала, за базата на анализирания сигнал се получава:

$$B = \Delta F.T = \frac{2}{\tau_0}.15.\tau_0 = 30$$

което доказва принадлежността му към сложните, шумоподобни сигнали.

Литература:

1. Варакин Л.Е Шумоподобные сигнали в системах передачи информации. М., Радио и связь, 1985
2. Винокуров В.И., Ваккер Р.А.: Вопросы обработки сложных сигналов в корелационных сигналов в кореляционных системах М. Сов. Радио, 1972
3. Ипатов, В. П., Камалетдинов, Б. Ж., Самойлов, И. М., Дисретные последовтельности с хорошими кореляционными свойствами, Зарубейная радиоэлектроника, 1989, № 9, с. 3 – 13

СТУДЕНТСКО-ДОКТОРАНТСКА СЕКЦИЯ

ФИРМЕНА ПОЛИТИКА „ДОНЕСИ СВОЕТО УСТРОЙСТВО“ И ОСИГУРЯВАНЕ НА ОБЛАЧНО БАЗИРАНИ УСЛУГИ

Андриана И. Иванова, Петър С. Великов

9021 гр. Варна, ул. Тепляков 4
E-mail : peter.velikov@gmail.com, andr.ivanova@gmail.com

BRING YOUR OWN DEVICE (BYOD) AND SECURING THE CLOUD

Andriana I. Ivanova, Petar S. Velikov

***ABSTRACT**: This report focuses on two trends - BYOD and Cloud computing. These trends alter security area, concepts and architecture of data protection. The purpose of the report is to highlight some of the new threats, understanding the concepts of protection and to assess in which cases it is appropriate to apply BYOD and Cloud services.*

***KEY WORDS**: BYOD; end node problem; cloud computing; fraudulent resource consumption; virtual machine security; side channels.*

Говорейки за новата парадигма за сигурност в киберпространството, трябва да разгледаме няколко основни тенденции, които променят начина на работа на компаниите. Тези тенденции изискват промяна в архитектурата и концепциите за защита. Ако приемем като твърдение, че до скоро осигуряването на сигурност се изграждаше в определен периметър на принципа „моят офис - моята крепост“, то в момента този модел търпи промени.

Вече можем да отбележим прехода от app-client модел към claud модел като факт. App-client модела губи позиции, защото трудностите със синхронизирането и актуализирането на приложенията върху множество устройства не задоволява потребителите. Клауд услугите от своя страна не изискват никакви усилия от страна на потребителя и са винаги на разположение при повикване, лесен достъп до виртуални машини или ресурси за съхранение.

Организациите и потребителите използват все повече облачно базирани услуги и приложения. Ще разгледаме видовете облаци и техните предимства, недостатъци и спецификации. Друга интересна тенденция, която променя IT бизнеса е полити-

ката Bring your own device (BYOD). Тази политика набира все по-голяма популярност и е пряко свързана с ползването на собствени устройства от работниците и достъп до работните ресурси. BYOD е възможна само и единствено благодарение на cloud модела. Чрез тази идея организацията използва по-ефеткивно хората с които разполага, като не ги ограничава пряко в офис среда и им позволява свобода на движение и възможност за работа извън офиса.

В доклада се спираме на две тенденции, а именно BYOD и Cloud computing, които променят пространството, модела, концепциите и архитектурата на защита на данните. Целта на доклада е да се отбележат заплахите, които пораждат тези тенденции, разбиране на самите концепции за защита и да се направи преценка, в кои случаи е удачно да се прилагат BYOD и Cloud услуги.

С BYOD се направи значителен пробив в света на бизнеса, тъй като около 75% от работниците и служителите в големи развиващи се пазари използват тази политика. Процента на ползване на собствени устройства в развитите пазари е около 44%. В повечето случаи, фирмите просто не могат да блокират тенденциите и се съобразяват с тях. Някои вярват, че BYOD може да помогне на служителите да бъдат по-продуктивни. Други твърдят, че тя повишава морала на служителите и предлага удобство да работиш със собствените си устройства и също така прави компанията да изглежда като гъвкав и привлекателен работодател. Тази практика се прилага най-вече в Близкия Изток като ползването й представлява около 80% от световното ползване на BYOD. Според изследване на Logicalis [7], пазари с висок растеж (включително Бразилия, Русия, Индия, ОАЕ и Малайзия) показват много по-висока склонност за прилагане на BYOD.

Някои индустрии възприемат BYOD по-бързо от други. В проучване от Cisco партньори [5] от 2013 г. относно практиката BYOD се твърди, че 9 от 10 американци използват собствените си смартфони за работа, 40% не използват парола за защита на смартфона си, 51% използват незащитени мрежи и само 52% изключват Bluetooth режима си. В образователната индустрия има най-висок процент на хората, които използват BYOD за работа около 95.25%. В проучване на IBM [9] се твърди, че 82% от служителите смятат, че смартфоните играят решаваща роля в бизнеса. Проучването също така показва ползите от BYOD включват повишаване на производителността, на удовлетвореността на служителите и намаляване на разходите на компанията. Повишената производителност идва от това, че потребителя лесно навигира и се чувства по-удобно с неговото лично устройство. Освен това, личните устройства често са най-новата дума на техниката, докато подновяване на технологиите и устройствата в дадено дружество не се случват толкова често. Удовлетвореността на служителите идва и от това, че те сами правят своя избор за ползване на дадена технология, а не им се налага технология избрана от IT отдела. Ако не се прилага BYOD политиката, всеки служител има съответното устройство за работа и за лично ползване т.е. два телефона, два таблета, два лаптопа и това създава неудобство. Споменатото по-горе може до доведе и до намаляване на разходите на компанията, защото тя вече няма да е отговорна за оборудването на служителите си.

BYOD обаче представлява едно огромно предизвикателство за сигурността на информацията. Проблемите със сигурността на BYOD са пряко свързани с проблема на крайния възел (end node problem) [8]. Проблема на крайния възел възниква когато личен компютър се използва за работа с поверителна фирмена информация

и временно става част от мрежата или облака на фирмата, а след това се използват в несигурни мрежи. Крайните възли обикновено имат слаб/остарял софтуер, слаби инструменти за защита, лесно можете да получите права за достъп до такова устройство, лошо конфигурирани са, имат инсталирани съмнителни приложения и софтуер и представляват реална опасност за неоторизиран достъп до чувствителната информация на даден бизнес.

BYOD води и до много тривиални проблеми. Например, ако един служител използва смартфон за достъп до мрежата на компанията и след това изгуби този телефон, трета страна би могла да извлече някакви незащитени данни от телефона. Друг вид нарушение на сигурността е налице, когато служител напуска компанията. Лицето обикновено не може да бъде принудено да върне устройството, така че приложенията на компанията и други данни, остават на него. Един от ключовите въпроси на BYOD, който често се пренебрегва, е проблема за телефонния номер. По-точно собствеността на телефонния номер. Въпроса възниква, когато служителите в отдел продажби или други подобни позиции ориентирани към клиента, напускат компанията и вземат телефонния си номер с тях. Клиентите след това се обаждат на номера и се оказва, че вече са при конкуренцията. Това води до преки загуби за компанията.

Нашите препоръки спрямо прилагането на BYOD политика, са:

- да се изготвят еднозначни клаузи в работните договори на всеки служител, за да не възникват спорове за собствеността. В договора ясно трябва да бъдат посочени всички задължения на служителя;
- да се поставят ясни критерии и стандарти за работа и защита на информацията;
- да се правят периодични проверки дали тези стандарти се спазват;
- да се провеждат периодични фирмени обучения на тема сигурност, както и обучения пряко свързани с BYOD политиката;
- може да се поставят и конкретни изисквания към устройствата.

Цялата BYOD концепция е положена на идеята за ползване на услуги и споделяне на информация в клауд среда. Ползването на услуги най-често става през браузър с цел уеднаквяване на предлаганата услуга за всички устройства.

Миграцията на информацията и на процесите към облачни структури променят не само мястото на което ползваме тези услуги, а променят фундаментално начина на работа. Облака решава много проблеми като върхови натоварвания, консолидация на данни, съхранение на големи масиви от данни и инсталиране на софтуерни актуализации, но новата технология също така създава нови предизвикателства в областта на сигурността и собствеността върху данните, трансграничната концепция за съхранение на данни, както и нуждата от обучение на висококвалифицирани професионалисти в тази специфична област. Тъй като все повече корпоративните и академичните среди инвестират в тази технология, работната среда на ИТ професионалистите също се променя драстично.

Най-основният фактор в развиването на клауд технологиите е публичния сектор. В условията на икономическа криза, правителствата по цял свят предпочитат да залагат на клауд технологиите, защото са по-евтини. Облачните структури им дават възможност да съкратят ИТ разходите наполовина. Не може да се отрече предимството на клауд технологиите за достъп и консолидиране на огромни обеми от данни, което ги прави изключително удобни за публичния сектор - администрацията и здравеопазването.

Например бившия CIO (Chief Information Officer) Вивек Кундра от администрацията на Обама, ще се запомни с политиката си "Claud first" [10], чрез която той твърди, че много от отделите в администрацията са намалили драстично ИТ разходите си. Този модел е национален приоритет и на Великобритания [2].

Въпреки че е прието, че едно от най-големите предизвикателства на клауд технологиите е сигурността, трябва да уточним какви точно заплахи съществуват и дали те са типични за облака и още по-точно, за коя разновидност на облачната реализация.

В доклада се разглеждат спецификите на public cloud модела, защото при private cloud модела са валидни всички стандартни методи за защита на даден периметър и оторизиране на достъп. Въпреки това според защитената теза на Джейсън Блумберг в неговата нова книга "*The Agile Architecture Revolution: How Cloud Computing, REST-Based SOA, and Mobile Computing Are Changing Enterprise IT"*се изтъкват 10 аргумента в полза на публичните облаци [3]. Що се отнася до Hybrid cloud реализацията, тя напрактика представлява реализация на два или повече клауда например (private, community or public). Пазарът на облачният компютинг може да се обобщи с една дума – хибриден облак. "2013 беше годината, когато производителите въведоха своите хибридни облачни стратегии, а 2014-а се очертава да бъде годината, когато потребителите ще започнат да ги използват. Според Gartner почти половината от големите предприятия ще ползват комбиниран публичен/частен облак, често описван като "хибриден" облачен компютинг до 2017 г." [4].

Европейската мрежова и информационна агенция за сигурност (ENISA) казва, че изчислителните облаци имат силно абстрактни архитектури и ресурси, почти мигновена мащабируемост и гъвкавост, почти мигновено доставяне, споделени ресурси, обслужване на търсенето, и програмно управление.

Националният институт по стандарти на САЩ и технологии (NIST) също е публикувала определение за облак: Облачният компютинг е модел позволяващ повсеместно, удобен, при поискване (OnDemand), мрежов достъп до общ изчислителен и конфигурируем ресурс (например, мрежи, сървъри, пространство за съхранение, приложения и услуги), които могат да бъдат бързо доставени и освободени с минимални усилия, както и да бъдат измерени предоставените услуги. Определението на NIST изброява пет характеристики от съществено значение за облаците, а именно ресурсите се предоставят по заявка, те са самообслужващи се, изискват мрежов достъп, използват споделени ресурси, притежават бързина и еластичност и могат да бъдат измервани. NIST също изброяват трите вариации на предоставяните услуги: (Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)). Те също очертават пет основни роли - потребител, доставчик, брокер, одитор и носител.

След разглеждането на тези термини и дефиниции, можем да започнем да разглеждаме потенциалните трудности, които възникват породени от архитектурата на клауд средата. Съществува security control framework - Cloud Security Alliance (CSA), създаден от ENISA и NIST , който е изготвил 98 правила за сигурност, които обаче не са актуализирани и по-скоро служат като препоръки отколкото да оказват някакъв контрол.

Въз основа на горепосочените роли и спецификации в облака, могат да възникнат следните проблеми:

- брокери - тази роля може да създаде проблеми за сигурността, в случай че облака изпълнява два типа услуги едновременно например SaaS и IaaS. Всъщност и двете услуги са пряко зависими от инфраструктурата, и при високо ниво на обещани ресурси, може да се достигне до невъзможност за обслужване на заявените параметри.

- при повикване - тази характеристика предполага предизвикателства за сигурността, свързани с бизнес потребителите, които лесно и моментално могат да заявят и да получат нови изчислителни ресурси, които трябва да се подсигурят предварително т.е. тази характеристика е пряко свързана с брокерите.

- споделено ползване на ресурси – атаката срещу един потребител, може да навреди на друг потребител, който ползва същите споделени ресурси. Възможността за наемане на услуги от различни потребители с общ споделен ресурс в даден периметър също представлява опасност. Този модел излага данните в споделения ресурс на опасност, а при PaaS и IaaS има и споделяне на изчислителен ресурс, което може да доведе до нападане на потеребителите помежду им, както и атака срещу целия облак.

- IaaS – при този модел виртуализацията играе главната роля при защита от злонамерени потребители в облака.

- широк мрежови достъп – тази харектеристика променя напълно модела за сигурност, който трябва да може да отчете, евентуално неблагонадеждни клиентски устройства.

- отчитане - тази характеристика разкрива нуждата от следене на заетостта на облака и отчитане на използваните ресурси от всеки потребител. Евентуална грешка в отчитането на ползването на даден ресурс би разколебало потребителите и би направило облака нерентабилен.

Основен проблем на публичните облаци е недоверието на клиентите към тях. Клиентите не искат да предоставят софтуера и поверителни данни в облак и да се доверят напълно, че тази информация се пази строго. Друг проблем е различните нормативни уредби в различните държави. Например това поставя въпроса дали данните в облака могат да бъдат одитирани от властите на държавата, където физически се съхранява информацията.

Атаки срещу бюджета - характеристика на публичните облаци е таксуването на ползвана услуга. Клауд доставчиците като Amazon EC2, Google Cloud Platform и Rackspace, таксуват US$0.09-0.08 на Gbyte (до 40 Tbytes - Egress). В масовия случай корпорацията си наема публичен облак и в него разполага уеб сайта си, уеб услугите и електроната си търговия. Облачно базираните услуги са уязвими на distributed denial-of-service(DDoS) атаки. Напрактика това са атаки създаващи изкуствен трафик на уеб услуги с цел забавянето им или претоварване на сървърите. Тези атаки са добре познати и съответния риск е добре проучен, но ще се спрем на една по-коварна атака. Съществуват атаки, които се стремят да използват модела на ценообразуване. Например чрез ботнет може да се изпълнява измамно потребление на ресурси (FRC *fraudulent resource consumption*) като по този начин много бързо клауд услугата може да се превърне в разорителна. Тези атаки се осъществяват изключително лесно и могат да бъдат изпълнявани от всяко свързано с интернет устройство. Например чрез Perl или JavaScript изпълняващи HTTP GET заявки. Уеб услугите на атакуваната компания отговарят на тези заявки и генерират трафик. За да онагледим тази заплаха, представете си 250,000 възли на ботнет, които могат да

изпращат по 3 заявки на секунда, при цени $0.09/Gbyte. Това може да доведе до колосални разходи на седмица. А също така този ботнет може и да изпраща заявки само два пъти дневно, така че да не можете да забележите лъжливия трафик.

Защитата срещу FRC атаки се базира на 4 основни задачи: предотвратяване, разкриване, разпознаване и смекчаване на последиците.

1. Предотвратяване – използването на автентикация би свело до минимум тази заплаха, но ние не го отчитаме като възможност, защото говорим за общия случай и за публикуване на общо достъпна информация. Поставянето на графични пъзели също са опция, но не всички хора са способни да попълват такива пъзели, и трябва да се внимава да не се дискриминират незрящите хора например. Други потребители нямат желание да попълват подобни пъзели. Третият вариант е да се следи за наличието на еднакви или подобни заявки и техните следи в мрежата. По този начин се повишава и възможността за разкриване на атаката.

2. Разкриване – не само честотата на заявките могат да ви помогнат да разкриете ботнет атака. За тази цел трябва да се вземат под внимание логовете на уеб сървъра и по-точно общия брой запитвания към уеб сайт от клиент. Чрез три параметъра: the Spearman, Overlap and Zipf metrics, можете да създате модел на нормалното поведение на сайта и после да откроите аномалиите.

Най-класическия метод да разберете, за съмнително повишено на потребление е да си следите сметката максимално често.

3. Разпознаване - предизвикателството в тази област е да се сведе до минимум броя на лъжливо идентифицирани реални клиенти. Това пряко спомага и за откриване на лъжливите клиенти. Последните изследвания показват, че нормалното поведение на клиента може да се характеризира с действията му като обем заявки, заявки на уеб документи и параметри от Web сесиите (заявки на сесия и брой сесии). Създаването на една добра статистика ще улесни справянето с FRC атаките. Естествено препоръчваме да информирате клиентите си, че следите броя на сесиите и за закачането на всякакви маркери и бисквитки.

4. Смекчаване на последиците – често е възможно завишената активност на даден клиент да ви заблуди, че той е злонамерен. Препоръчваме да не го включвате в черния списък веднага, а да включите защита с графичен пъзел.

Като цяло всички проблеми с “Utility model” на клауд услугите могат да бъдат генерално решени от клауд доставчиците, но към момента доколкото е известно на авторите, това не се прави. Със сигурност няма кой да изгради по-добри статистики и системи за защита освен самите доставчици по вече споменатите принципи за следене на трафика.

Заплахи в облака – идеята на публичния облак е софтуера на дадена компания да работи върху сървърите на друга компания с възможност за ползване на информация (или уеб съдържание на потребители) от трета компания. Това естествено създава риск за информацията.

Вместо да си купят или да си наемат сървъри, разработчиците на Instagram разположиха цялата услуга, използвайки под наем инсталация на популярната EC2 на Amazon - (EC2 е краткото наименование на Elastic Compute Cloud) [1]. Въпреки, че в Instagram ползват криптография като Secure Sockets Layer (SSL) и Secure Shell за да запазят данните на потребителите си, възниква въпроса къде се съхраняват публичния и съответно тайния ключ за тази информация. Те са на хардуер, върху който Instagram нямат контрол.

Cloud платформите, обаче преплитат потребителските задачи върху споделен ресурс. Повечето потребители не знаят за това преплитане, защото клауд доставчиците изолират всеки клиент на отделна виртуална машина. На теория отделната виртуална машина би трябвало да изолира и информацията. Но що се отнася до криптографията, някои проучвания сочат, че съществуващата защита може да се окаже недостатъчна. Учени от University of North Carolina, RSA Laboratories и University of Wisconsin [6], демонстрираха как можеш да извлечеш криптографски ключове от една виртуална машина в друга, дори и всички стандарти за клауд защита да са спазени. Това е възможно заради Side channels. Тези атаки са добре познати и са изиграли основна роля в историята на криптографията. Те могат да възникнат при извънредни обстоятелства като електромагнитни излъчвания, потребление на електричество (прави се анализ т.е. следи се промяната на консумация на ток на процесора по време на алгоритъма и се установява дали процесора умножава или не, което води до прочитане на битовете), които да бъдат използвани за пробив.

Клауд средата е изключително благодатна за потенциални side channels, защото различните виртуални машини споделят общи физически ресурси например: процесор, кеш с инструкции или диск на един физически компютър. Ако една атакуваща програма може да следи поведението на тези ресурси, то теоретично може и да определи какво друга програма прави с тях. Тази теория е отдавна дискутирана и доставчиците на клауд услуги я отхвърлят базирайки се на практиката. Те твърдят, че на един сървър използват много повече от две виртуални машини, което изключва възможност за следене на ресурсите. Освен това The Virtual Machine Manager (VMM) software, слага допълнителни бариери между атакуващия потребител и ресурсите на останалите потребители. Още повече, че отделните виртуални машини са често разменяни между различните ядра на многоядрените сървъри, което още повече затруднява следенето на ресурсите.

Учените публикували статията са се спрели на Xen VMM. Това е софтуера, който Амазон ползват за EC2. Експеримента не е проведен на EC2, а на подобен хардуер – многоядрен сървър, но с изключен многонишков режим(simultaneous multithreading (SMT)). При експеримента атакуващата виртуална машина и жертвата са на един физически компютър и жертвата декриптира с Elgamal ciphertext използвайки libgcrypt(GnuPG). Elgamal е чудесен пример за side-channel атаки, защото лесно може да се декриптира присвоения ключ (ciphertext). Тази атака е възможна, само ако атакуващата виртуална машина следи точно за състоянието на хардуера. Тези атаки следят и за cache пропуски в споделената кеш с инструкции. При този вид атака, първо атакуващия виртуален компютър заема кеш паметта с определени инструкции, след което изчаква неговите кеш блокове да започнат да се изместват от целта (т.е. друг виртуален компютър). Според това, кои блокове на кеша са изхвърлени от кеш паметта, може да се определи каква операция извършва целта на атаката. За да успее атаката, атакуващия компютър трябва да си върне управлението върху кеш паметта възможно най-бързо и да провери, кои кеш блокове са били изхвърлени изпълнявайки същите инструкции и записвайки времевите резултати. Ако някой блок е бил освободен от кеш паметта ще се получи кеш пропуск и ще възникне определено забавяне. Тук най-трудния момент е връщането на контрола бързо. По принцип Xen и VCPUs не позволяват мигновеното връщане на контрола, но има изключения. VCPUs дава приоритет на виртуални процесори получаващи прекъсвания. Изследователите са успели да постигнат целта с помощ-

та на два процесора, като задачата на втория процесор е била само да предизвика прекъсване. Използвайки този метод връщането на контрола върху кеша отнема около 16 микросекунди. Това наистина е много процесорно време, но е достатъчно кратко за да даде полезна информация. На изследователите се е наложило да приложат и алгоритъм за отчитане на различните инструкции изпълнявани от целтта, както и изключването на възможността да попаднат в ядрото на операционната система или изобщо да объркат виртуалната машина. Приложили са и hidden Markov model, и в крайна сметка са успели да достигнат до успех. След няколко часа работа са успели да съберат около 1000 фрагмента от ключове, от които около 330 са били достатъчно дълги за да се реконструират.

Този експеримент единствено доказва теоритична несигурност. Трябва да се отбележе, че има далеч по-надеждни криптиращи протоколи (OpenSSL и RSA). Освен това експеримента е проведен само с две виртуални машини и с предварително въведени данни за хардуера. И най-важното за да можете да атакувате дадена виртуална машина, трябва да успеете да разположите вашата в същия физически сървър.

Нашите препоръки при избора на клауд са:

- да се изгради стратегия за преминаване към облачно базирани услуги;
- според особеностите на бизнеса да се определи коя спецификация и клауд реализиация е подходяща;
- при изграждане на стратегията да се определи кои услуги могат да се пуснат като публични;
- да се направи преценка дали тази услуга ще се развива и ако е така да се вземат предвид възможностите за персонализация (цени, време) в public cloud.
- да се оценят финансовите параметри за реализация на услугата в публичен клауд или вътре в компанията.

Според изложеното в доклада и посочените проучвания тези две тенденции са част от настоящето и бъдещето ни. Те променят не само корпоративната среда, а дори и нагласите и изискванията на всеки служител. Това неимоверно води до промени в концепцията за информационна сигурност.

Авторите на доклада се присъединяват към мнението на Джейсън Блумберг, че публичните облаци изплозват най-новите технологии, те са по-икономични и по-гъвкави, публичните облаци привличат най-добрите специалисти по информационна сигурност, периодично се провеждат тестовете за защита от несанкциониран достъп и по този начин решават проблемите със сигурността.

Източници:

1. http://aws.amazon.com/ec2/
2. http://cio.bg/5383_oblacite_veche_sa_nacionalen_prioritet_za_velikobritaniya
3. http://cio.bg/5480_10_predimstva_na_publichnite_oblaci
4.http://cio.bg/6357_hibridnite_oblaci_godinata_na_masovoto_im_vazpriemane_e_pred_nas
5.http://www.ciscomcon.com/sw/swchannel/registration/internet/registration.cfm?SWAPPID=91&RegPageID=350200&SWTHEMEID=12949
6.http://www.computer.org/cms/Computer.org/ComputingNow/CloudPrototype2013/2013_IEEECloudComputing_Prototype_LoRes.pdf
7. http://cxounplugged.com/2012/11/ovum_byod_research-findings-released/
8. http://en.wikipedia.org/wiki/End_node_problem

9. http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html
10. http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

СИСТЕМИ ОТ ТЕХНИЧЕСКИ СРЕДСТВА ЗА ПОЛУЧАВАНЕ НА РАЗУЗНАВАТЕЛНА ИНФОРМАЦИЯ ОТ КОМПЮТЪРНИ МРЕЖИ

Христо А. Десев
Свилен С. Камджалов

Национален Военен Университет " В. Левски" гр. Велико Търново
Факултет "Артилерия ПВО и КИС" гр. Шумен

SYSTEMS OF TECHNICAL MEANS OF OBTAINING INTELLIGENCE INFORMATION FROM A COMPUTER NETWORK

Hristo A. Desev
Svilen S. Kamgalov

ABSTRAKT: *The main purpose of the funds for technical intelligence is through them to draw information. In the modern world the technical resources it uses are different intelligence and high efficiency, this is why protection of information must adopt an adequate form of countermeasures.*

KEY WORDS: *technical resources, protection, information reliability.*

Развитието на техника, на информационните и телекомуникационните технологии, както в света, така и у нас, довежда до неимоверно увеличаване броя на различните видове приложения и съответно - до интензивно нарастване на трафика на предаваните данни по обществените и корпоративните мрежи. Увеличава се броят и обемът на базите данни, достъпът до които се осъществява чрез мрежите. Информацията, която е класифицирана, е главна цел на защита от контраразузнаването.

Техническите средства за разузнаване са неделим елемент от въоръжения потенциал на всяка страна и са непосредствено свързани с неговата модернизация. Основната цел на средствата за техническо разузнаване е чрез тях да се черпи информация. В съвременния свят техническите средства, с които си служи разузнаването са различни и с висока ефективност, именно поради тази причина защитата на информацията трябва да приеме една адекватна форма на противодействие.

В закона за специални разузнавателни средства (СРС), като такива са обособени техническите средства и оперативните способи за тяхното прилагане, които се използват за изготвяне на веществени доказателствени средства – кинозаписи, видеозаписи, звукозаписи, фотоснимки и белязани предмети. "Технически средства са електронни и механични съоръжения, както и вещества, които служат за документиране на дейността на контролирани лица и обекти" [1].

В дейността на СРС от съществена важност са секретността и надеждността на функциониране, тяхната проява следва да се разглежда в няколко аспекта.

Енергийния аспект се определя от това доколкото наличието на специални технически средства (СТС) довежда до промяна на енергетичния стандартен фон, независимо от физическата форма на тази енергия – радиовълни, акустични, вибрационни полета или такива от оптическия диапазон. По същество това е способността СТС да функционира без енергийни излъчвания или с такива, които почти не променят съответния фон на мястото на действие;

Информационната надеждност и секретност са съотносими със степента на защитеност на канала за трансфериране на информацията от случайно прихващане отвън и разшифроване на прихванатата вече контролируема информация.

Физическата защитеност зависи от степента на различие на каналът за изтичане на информацията по физически и физико - химически характеристики (съдържание на метали; плътност на масата или електронна плътност; наличие на полупроводници, вълнови съпротивления) от околната среда. Физическата защитеност често може да се разглежда като съставна от елементи, в зависимост от това какви физични, физико-химични и даже физиологически характеристики притежават. Физическата защитеност е висока, когато каналът е хомогенен, слива се с околните особености на пространството. Тя с нейните специфични съставни – помещения, канали за връзка, определят тактическата класификация на специалните технически средства.

Системите за следене на трафика от данни, използвани от разузнавателните организации, представляват съвкупност от основно три програми – "снифер" с филтър, който да избира кои пакети са "интересни" (много е важно да има добър критерий за филтриране), програма която да може да “сглобява” отделните пакети и програма която да представя уловените данни в подходяща за използване форма. Събраната информация от системата би трябвало да има за цел да се използва при нужда, затова събирането на данни трябва да отговаря на строги изисквания, за да е възможно използването й като доказателство. За да се използва ефективно подобна система трябва да има законова основа за това, която да задължава ISP да предоставят достъп до мрежата си. По – проблематичен е въпроса как ще се накара една частна фирма да предостави възможност да се подслушват служителите й.

В основата на всяка система за подслушване на трафик е обикновен снифер. Пакетният снифер е хардуерно устройство, закачено за самия кабел, или софтуер, който подслушва мрежовия трафик в съответния мрежов сегмент. Ако в мрежовият сегмент няма суич (switch), всички пакети се доставят (broadcast) до всички компютри в мрежата, но само тази със съответния MAC адрес, който идентифицира еднозначно съответния мрежов интерфейс и приема съобщението. Всички останали компютри виждат съответния пакет, но го игнорират. Когато на компютри се използва снифер за подслушване на трафика в мрежовия сегмент, е необходимо мрежовата й карта да е в режим на приемане на всички пакети (promiscious mode). Проблемът идва от това, че ако компютъра, е врязана към суич, то трафика на пакети се управлява от суича. Всеки пакет ще се изпрати директно към компютъра-получател, без пакетът да се изпраща до всички останали. Един кракер би избегнал този проблем, ако използва методи като ARP/MAC spoofing и др. Сниферите са широко разпространени сред администраторите на мрежи за анализиране на трафика и диагностика на проблеми в мрежата им. Използват се и от кракери за добиване на неправомерен достъп до информация. Сниферите представляват проблем

за сигурността, когато се използват неправомерно, защото е много трудно да се разбере, че в мрежата е включен снифер, тъй като обикновено те не генерират трафик. За откриване на снифери се използват методи, използващи в основата си ICMP Echo Request или ARP Request заявки, други разчитат на това, че много снифери правят reverse – DNS запитвания, трети пък разчитат на латентност, и т .н. Като цяло няма сигурен метод за тяхното откриване. Изследваната система използва опростен снифер, тъй като със силата на закон е гарантирано съдействието на ISP- то. Тя се свръзва към подходящ мрежов сегмент, през който минава трафика на интересуващия ни потребител (или жертва?). Поради тази причина разузнавателните служби нямат нужда да прилагат разни кракерски трикове. Тъй като подслушвателната система трябва да чете всички хедъри на пакетите, трябва да се внимава къде тя се вързва към мрежата на ISP, защото при невнимателен избор на подмрежа може да се получи "забиване" (denial of service) на системата при четене на прекалено много хедъри.[2]

Филтрирането на трафика е началната стъпка и е много е важно да се прилагат добри критерии за филтриране, с цел предпазване на системата от претоварване.

- филтриране по фиксирано IP - това е най - простия метод, при който единствено трябва да се въведе съответния IP адрес (или множество от IP адреси). Използване на филтриране по множество от IP адреси (например на една подмрежа с 255 хоста) трябва да се прави с повишено внимание, защото може да се окаже че данните, които трябва да се запазят са прекалено много;

- филтриране по динамично IP – при невъзможност за филтриране по фиксирано IP, може да се използва динамично филтриране. Обикновено за динамично задаване на IP адреси се използват протоколите DHCP (Dynamic Host Configuration Protocol) или RADIUS (Remote Authentication Dial In User Service). За DHCP, MAC адресът трябва да е известен, а за ADIUS трябва да е известно и потребителското име, с което потребителят е регистриран в базата данни на RADIUS Софтуерът за RADIUS сървър съдържа три части: сървър за аутентикация, клиентски протоколи и сървър за таксуване. RADIUS сървърът проверява дали информацията е коректна, като използва аутентикационни схеми, като PAP,CHAP или EAP. Ако информацията е приета, сървърът предоставя достъп до системата;

- филтриране по протоколи - за всеки от основните протоколи (TCP, UDP, ICMP) трябва да има възможност за избор дали да се приемат пакети предадени по определен протокол и какъв да бъде режимът на запис.

- филтриране по текст – изпълнява се заявка за всички TCP пакети от дадено IP, като в пакетите се среща думата "FBI". Друга възможност е да се записват TCP сесията на потребителя, след като е открита определена дума в трафика му. Тук трябва да се внимава в каква кодираща схема използва потребителят (ASCII, Unicode, BASE, UUENCODE) за да може търсенето да бъде ефективно при криптиране на кореспонденцията, този метод за филтриране е безполезен.

- филтриране по порт - тази възможност е полезна, ако искаме да проверяваме, примерно, само пощата на потребителя. Тогава трябва да изберем филтриране на TCP портове 25 и 110 (съответно за SMTP и POP3). Ако искаме да записваме сайтовете, които посещава – филтрираме TCP порт 80. Естествено, това са стандартните портове за тези услуги и няма гаранция, че не са променени. Например, често срещано е HTTP да е пренасочен към порт 8080.

- филтриране по *email* адрес - този метод за филтриране се слуша за SMTP или POP3 трафик и се следи дали email адресът съвпада с желания (или желаните). Една съвременна система трябва да позволява използване на различни групи от филтри за по – гъвкаво и ефективно отсяване на ненужната информация

Едни от най-важните изисквания към системата е гарантиране на недостъпността й от неоторизирани лица и невъзможност за манипулация на събраните данни, дори и от агенти на разузнавателната служба. Към последното изискване е наложително да се добави и това, че трябва да има реализирана система за аутентикация на потребителите (агентите). Желателно е за това изискване да се избере подходяща операционна система с вградени такива възможности.

Друга жизнено важна характеристика на подобна система е независимост на електрозахранването й. Това ни подсеща, че е необходимо да има и някакъв начин за индикиране на пропуснати пакети. Един начин това да се направи е като се следи информацията в хедърите на пакетите. Пропускане на пакети може да се получи или при спиране на системата или при прекалено голям трафик. Както вече споменахме, необходимо е системата да се свързва към мрежов сегмент, по който трафикът е възможно най-малък и вътрешните буфери на системата да са съобразени с очаквания трафик. Пропускането на пакети крие още по-голяма опасност при използване на динамично зададени IP адреси. В този случай системата може да пропусне отписването (sign – off) на подслушвания субект от мрежата и да се продължи с подслушването на друг потребител, който междувременно е заел съответния IP адрес.

Други технически характеристики са наложени от факта, че събраните данни трябва да се използват от съдебната власт. Затова е задължително системата да притежава два основни режима за събиране на данни;

– режим при който само се регистрира комуникацията на подслушвания субект (pen mode). Наложително е да се обърне внимание, че не целите хедъри трябва да се запазват, защото някои от тях съдържат информация за съдържанието на пакета (неговата дължина, дали е текст, картинка, аудио и др.), което може да влиза в нарушение със съдебните разпоредби;

– пълният – записва се всичко. Причината за това разграничаване се дължи на факта, че разрешение за подслушване в pen mode се взима много полесно и бързо (информацията, която се събира е същата като при послушване на телефона). При експлоатиране на една такава система за подслушване, най – вероятно ще има нужда тя да се управлява централизирано, което веднага ни изправя пред въпроса за нейната сигурност.

Системата за подслушване на трафик може да е изградена от няколко машини, което налага строга синхронизация на времето с всички машини в системата. И последна, но не маловажна подробност е нуждата от синхронизация с ISP – то относно протоколите и техните версии, които се използват. Това е наложително за да може да се извършва прецизно филтриране и да не се окаже, че системата не може да прочете правилно хедърите. [4]

Да проследим как тези безспорно важни изисквания са реализирани в една реална система за подслушване на мрежов трафик, която се е използвала в САЩ от ФБР, а именно "Carnivore".

Цялата система за следене на трафика, използвана от ФБР се състои от три сегмента-програми:

- Carnivore - за събиране на пакетите;
- Packeteer - за реконструиране на пакети от данните, предадени от Carnivore;
- Cool Miner, която служи за представяне на“улова”в подходящ за четене вид. Цялата система е наречена Dragon Ware Suite.

Carnivore се инсталира без монитор и клавиатура и по време на работа не може да се добие физически досъп до него. Всеки Carnivore е оборудван и със стандартен 56 kbps модем и се свързва към специално създадена телефонна връзка. Контролният компютър се свързва към събиращия компютър посредством телефонна връзка. На контролния компютър е инсталиран комерсиален софтуер pcAnywhere на Symantec, чрез който се контролира събиращия компютър. Софтуерът поддържа аутентикация и всеки, който използва програмата има потребителско име и парола. За защита на комуникацията, pc Anywhere използва симетрично криптиране на данните (това не е класическото симетрично криптиране, а вариант на Symantec, който има и компонент public-key при задаването на симетричния ключ).

Софтуерът Carnivore е разработен от експерти на ФРБ и се използва до 2005 г., когато е заменен с по-ефективна комерсиална програма, която има аналогични функции. Въпреки че служителите на федералното бюро официално го наричат "инструмент за мрежова диагностика", той има доста по-широко предназначение. Продуктът се инсталира на сървърите на даден интернет доставчик и на практика следи целия мрежов трафик, който преминава през машината. Става дума дори за информацията, която се предава транзитно към мрежите на други провайдъри и по принцип се игнорира от въпросния компютър. Когато засече съмнителен мрежов пакет на базата на ключова дума или самоличността на изпращача, Carnivore копира информацията и я анализира допълнително. DCS - 1000 е система , базирана на Windows и е вградена както в търговски, така и в частен софтуер. Пътувайки по интернет „подушва” пакетите информация и копира тези, които търси.

Ровенето в електронните пощи и засичането на "съмнителен" мрежов трафик е основен приоритет на съвременните служби за сигурност. Двете най-известни инициативи в тази сфера са програмата Carnivore ("Хищник") на Федералното бюро за разследване (ФБР) и Echelon на щатската Агенция за национална сигурност (NSA). Най-нашумели са хакерските средства на федералните агенции като Магически фенер (Magic Lantern) и Key Logging. Магическият фенер е троянски кон , изпратен по електронната поща, който се инсталира в компютъра-мишена и прихваща всеки знак, написан от следения човек. Така разчита всяка парола и чрез нея отваря кодираните документи. Key Logging е старо средство, което ФБР инсталира при криминални разследвания , съгласувани със sneak-and-peak обиск.

Системата на подслушването прилага механични, електронни или други средства. Такива устройства са пишещ брояч (Pen Registers), прикрепен към телефонната линия, който записва номера на всеки телефон, набиран в линията и проследяващо устройство (Trap Trace Devices) (Pen/Trap). Използва се и Carnivire (DCS-1000), което селективно прихваща информация от интернет, обект на законова процедура и пропуска комуникациите, които не се наблюдават. ФБР широко разгласи съществуването на Carnivore на 11 юли 2000 година. Системата се инсталира на устройствата на интернетния доставчик и може да наблюдава и контролира целия трафик, който се движи през него. DCS -1000 е част от комплект от средства, познат като Dragon Ware, включващ Packeteer и Coolminer, които могат да възпроизведат уеб страници, точно както наблюдаваният ги вижда.

Поради големия натиск от организации за защита правата на човека и от медиите, ФБР се съгласява да се направи технически преглед само на част от системата Dragon Ware. Той е извършен от IIT Research Intitut и е официално публикуван на 8 декември 2000г.

Много по-драстични са мерките, които САЩ предприеха, за да увеличат своята интернет сигурност, особено след терористичните атаки от 11 септември 2001 г. Първите гласувани промени - USA Act (Uniting and Strengthening America) и Patriot Act (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism), позволяват на полицията да следи интернет трафика, без да има нужда от съдебна заповед, да се използва системата Carnivore (набор от програми за наблюдение на интернет - имейли, сайтове, чатове и предаване на информация от или към заподозрени), а ФБР да има достъп до всяка лична информация - медицинска, образователна, персонална кореспонденция и т.н.

В контекста на разгледаната в материала информация е важно е да се направи анализ на ефективността, причините за използване на голямо количество СРС от оперативните служби, свързани с обществения ред и сигурност, както и на вътрешното разпределение на използваните СРС по отделни способи. Възниква и въпросът за ефективността на подслушването на комуникациите – обществена тайна е, че само 2-4 % от СРС от тях влизат в съда. От разгледаното следва да се направят няколко извода:

1.Контролът на компютърната информация е превръща самостоятелен способ с нарастващо значение, предвид широката употреба на компютри и т. нар. кибернетизация на обществото. Нарастването на компютърните престъпления прави този способ особено актуален и необходим.

2. Основните насоки за реализация на този способ трябва да се насочат към:

- преодоляване на програмните средства за защита, чрез използване на различни методи за проникване до съхраняваната информация, използвайки слабите места на физическата защита и преодоляваните софтуерните системи;

- копиране на информацията от носители до които е възможен случаен или специално създаден достъп и прихващане на информацията в каналите за връзка.

3. Законово обезпечаване на обосновано и разрешено прилагане, както на отделните способи, технически средства, така също и на, резултатите, получени вследствие на приложението им.

ЛИТЕРАТУРА:

1. Закон за специалните разузнавателни средства, ДВ. бр.95 от 21 Октомври 1997г.

2. Crispin, Mark M., 2002 – What's Wrong With This Picture?, http://www.mediachannel.org/atissue/conflict/.

3. Smith Andrew F., 2002 – International Conflict and the Media, http://www.mediachannel.org/atissue/conflict/.

4. McChesney, Robert W., 2002 – Corporate Media, Global Capitalism, In Simon Cottle, editor, *Media Organisation and Production*. London: Sage.

5. Семерджиев, Ц. Информационна война, Изд. Софтрейд, С., 2000

6. Семерджиев, Ц. Управление на информационната сигурност – учебно пособие, Изд. Софтрейд, С., 2007

7. Колектив, Компютърна и мрежова сигурност, Унив. изд. Епископ Константин Преславски, 2005

МОДЕЛИ ПРИ УПРАВЛЕНИЕТО НА ИНЦИДЕНТИ В ИНФОРМАЦИОННАТА СИГУРНОСТ

Владимир П. Крумов

Национален военен университет „Васил Левски”
Факултет „Артилерия. ПВО и КИС”, гр. Шумен

MANAGEMENT MODELS COMPUTER SECURITY INCIDENTS

Vladimir P. Krumov

***ABSTRACT**: This report examined two models for managing events described in the international standard ISO 27035 standard and the U.S. in this area 800-61. A comparative characterization and shows the differences between the two standards.*

***KEY WORDS**: information security, incident, incident management*

В края на 20-ти и началото на 21-ви век сме свидетели на процес на глобализация, която наложи нови модели на общуване между хората и между институциите, в които широко приложение намериха средствата за масова комуникация .

Развитието на този тип комуникация предоставя редица предимства на хората за комуникация. Едновременно с това се появиха множество непознати до този момент рискове и заплахи, породени от уязвимостите на информационните ресурси, използвани от хората и организациите за осъществяването на връзка между тях. Все по – голямо значение за предпазване от неблагоприятни въздействия върху този тип комуникация придобива политиката за сигурност на информацията важна част от която е и политиката за управление на инцидентите.

За да характеризираме едно събитие като инцидент, то трябва да отговаря на следното определение [1] : отделно събитие или серия от нежелани или неочаквани събития, свързани със сигурността на информацията, които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информацията.

Политиката за управление на инцидентите са разгледани в няколко стандарта. Обект на разглеждане в този доклад са двата стандарта ISO 27035 “ Information technology — Security techniques — Information security incident management “ и стандарта на агенцията за национална сигурност на САЩ 800 – 61 издание 2 “Computer security Incicent Handling Guide”

В тези стандарти моделите при управление на инциденти са описани като действия включени в няколко фази:

При ИСО 27035 фазите са:

1. Документиране на дейностите
2. Откриване
3. Докладване
4. Оценяване
5. Реагиране

6. Извличане на поуки

При стандарта използван в САЩ фазите са по – малко и те са :

1 . Подготовка;

2. Откриване и анализ

3. Управление на риска

4. Извличане на поуки

Първите фази и при двата вида стандарта са подготвителни като при ИСО 27035 дейността е насочена към написване на политики за управление на инцидентите, докато при 800 – 61 освен създаване на политиките за управление на инцидентите се включват и дейностите за създаване и обучение на екип за реагиране на инциденти, както и придобиване на ресурси за това. По време на подготовката, организацията също така се опитва да ограничи броя на инциденти, които ще се появят чрез избиране и прилагане на набор от контроли въз основа на резултатите от оценките на риска които са правени до сега. Това се явява и разликата в тази фаза между 2 – та стандарта.

Следващите 3 фази при ИСО 27035 са обединени в една фаза при 800- 61 като дейностите описани в двата стандарта са идентични:

- дейност за откриване и събиране(документиране) на информацията по даденото събитие/инцидент;

- дейности по въздействието върху дадената заплаха;

- дейности, гарантиращи че правилно се събират и съхраняват доказателства за даденото събитие/инцидент и използването на тези доказателства в случай, че са необходими за съдебно преследване;

- дейности, гарантиращи че базата данни на информационната сигурност се поддържа актуална.

Първия начин за откриване на инцидент е при периодичните оценки на риска на системи и приложения . Тези оценки трябва да определят какви рискове са породени от комбинации от заплахи и уязвимости. Тази оценка трябва да включва както общоизвестните заплахи , така и известни специфични за организацията заплахи. Всеки риск трябва да бъде с приоритет , както и рисковете които могат да бъдат намалени , прехвърлени, или приеит , докато не се постигне разумно цялостното ниво на остатъчен риск. Други начини за откриване на събитие/ инцидент е след доклад от служител или от автоматизирана система за сигнализиране.

Дори да имаме информация за събитие, не означава непременно, че е настъпил инцидент. Някои показатели , като например проблем със сървъра или модификация на критичните файлове, може да се случи по няколко причини , различни от инцидент по сигурността , включително и човешка грешка . Като се има предвид наличието на показатели , обаче е разумно да се предполага, че даден инцидент може да настъпи и да действа по съответния начин .

Приоритизиране разглеждането на инцидента е може би най-критичната точка в анализа и взимането на решение в процеса на обработката на инцидента . Инциденти не трябва да се обработват по начина първи дошъл , първи обслужен в резултат на ресурсните ограничения . Вместо това, следва да се даде приоритет на базата на съответните фактори , като например следното :

- Поле на въздействие на инцидента . Инциденти , насочени към ИТ системи обикновено повлияят на бизнес функционалността на организацията. Също така

инциденти може да влияят върху поверителността , целостта и наличността на информация на организацията.

- Размер на инцидента и необходими ресурси за справянето с него. Размерът на инцидента и типа на ресурсите които го засяга ще определи размера на време и ресурси, които трябва да бъдат изразходвани за възстановяване от този инцидент . В някои случаи не е възможно да се възстанови дадената организация от инцидента (напр. , ако поверителността на чувствителната информация е компрометирана) и не би имало смисъл да се харчат ограничените ресурси за реагиране на инцидента, освен ако това усилие не е насочено към гарантиране, че подобен инцидент няма да се случи в бъдеще. В други случаи реагирането на инцидент може да изисква много повече ресурси, отколкото това, което организацията има на разположение.

При документирането на инцидента трябва да разполагаме със следната важна информация:

- Текущото състояние на инцидента (нова , в процес , предадена за разследване , решен, и т.н.)
- Обобщение на инцидента
- Индикатори, свързани с инцидента
- Други инциденти , свързани с този инцидент
- Действия , предприети от всички работещи с инцидента на този инцидент
- оценки на въздействието, свързани с инцидента
- списък на доказателствата, събрани по време на разследването на инцидента
- Следващи стъпки трябва да бъдат предприети

Следваща фаза и при двата модела е управлението на риска като и тук дейностите са сходни и при двата стандарта които са описани в процедурите в първата фаза с разликата, че при 800 – 61 са предвидени и дейности по възстановяване на системата към нормална работа след като инцидента е неутрализиран. Допълнителните дейности включват :

- премахване на компоненти на инцидента , като например изтриване на зловреден софтуер и блокирането на нарушените потребителски акаунти , както и идентифициране и смекчаване на всички уязвимости, които са били експлоатирани;
- възстановяване на системите заменяйки увредените файлове с чисти версии , инсталиране на кръпки , смяна на паролите , както и затягането на периметъра на мрежата за сигурност (например , защитна стена)

Последната фаза но не по значение и при двата стандарта е извличането на поуки. Една от най-важните дейности в тази фаза а също най- често пропускана е учене и подобряване на персонала, като се отразяват новите заплахи , подобрена технология , и извлечените поуки . Провеждане на "научените уроци " с всички заинтересовани страни , след сериозен инцидент , и евентуално периодично след по-малки инциденти, когато ресурсите позволяват , могат да бъдат изключително полезни за подобряване на мерките за сигурност и самия процес на работа с инцидента.

Актуализиране на политиките и процедурите за реагиране при инциденти е друга важна част от тази фаза. Следклиничния анализ на начина, по който се бори с инцидента често ще разкрие липсващ етап а или неточност в процедура , като създава стимули за промяна.

Друга важна дейност в тази фаза е създаване на доклад за проследяване за всеки инцидент , който може да бъде доста ценен за бъдеща употреба . Докладът предоставя препратка, която може да се използва, за да помогне при работа с подобни инциденти. Създаване на официална хронология на събития е важно за правни причини , като се създаде парична оценка на размера на щетите , причинени от инцидента.

Използването на описаните по- горе модели за управление на инцидентите води до следните предимства пред организацията:

- Подобряване на ефективността на мероприятията за защита на информацията. Това ще подобри цялостната сигурност като помага за бързо идентифициране и прилагане на съгласувано решение и по този начин осигурява средство за предотвратяване на бъдещи подобни инциденти по сигурността на информацията ;
- Намаляване на вредните въздействия върху бизнеса. Тези въздействия могат да включват незабавна финансова загуба и по-дългосрочна загуба, произтичаща от повредени репутация и доверие;
- Засилване на вниманието за предотвратяването на инциденти, включително и методи за идентификация на нови заплахи и уязвимости;
- Ефективност при оценяването и третирането на докладваните уязвимости по сигурността на информацията;
- Бързо извличане на поуки от възникналите инциденти.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. ISO / IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary
2. ISO / IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements;
3. ISO / IEC 27035:2011 Information technology — Security techniques — Information security incident management**;**
4. ISO / IEC 27005:2011 Information technology — Security techniques — Information security risk management
5. NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide 2012

НАУЧНА КОНФЕРЕНЦИЯ 2014

НОВАТА ПАРАДИГМА ЗА СИГУРНОСТ В КИБЕРПРОСТРАНСТВОТО

СБОРНИК НАУЧНИ ТРУДОВЕ

Българска. Издание първо. Тираж 30

Предпечатна подготовка във Факултет „Артилерия, ПВО и КИС“ - Шумен